Sumsets of reciprocals in prime fields and multilinear Kloosterman sums

J. Bourgain
Institute for Advanced Study,
Princeton, NJ 08540, USA
bourgain@ias.edu

M. Z. Garaev
Centro de Ciencias Matemáticas,
Universidad Nacional Autónoma de México,
Morelia 58089, Michoacán, México
garaev@matmor.unam.mx

Abstract

We obtain new results on additive properties of the set

$$I^{-1} = \{x^{-1} : \quad x \in I\}$$

where I is an arbitrary interval in the field of residue classes modulo a large prime p. We combine our results with multilinear exponential sum estimates and obtain new results on incomplete multilinear Kloosterman sums.

1 Introduction

In what follows, $\varepsilon > 0$ is an arbitrary fixed constant, $\mathbb{F}_p$ is the field of residue classes modulo a large prime p which frequently will be associated with the set $\{0, 1, \ldots, p-1\}$. Given an integer x coprime to p (or an element x from $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$) we use x^* or x^{-1} to denote its multiplicative inverse modulo p.

Let I be a non-zero interval in $\mathbb{F}_p$. Additive properties of the reciprocal-set

$$I^{-1} = \{x^{-1} : \quad x \in I\},$$

with a subsequent application to Kloosterman sums have been considered in [5]. Among other results, it has been shown there that for any $\delta > 0$ there exists $k \in \mathbb{Z}_+$ such that the sumset

$$k(I^{-1}) = \{x_1^{-1} + \ldots + x_k^{-1} : \quad x_i \in I\}$$

satisfies

$$|k(I^{-1})| > p^{-\delta} \min\{|I|^2, p\}.$$

In the most interesting case $|I| < p^{1/2}$ this implies that $|k(I^{-1})| > |I|^2 p^{-\delta}$. From some recent results in [12] (see Lemma 10 below) it follows that

$$|I^{-1} + I^{-1}| > \min\{|I|^2, \sqrt{p|I|}\}|I|^{o(1)}. \qquad (1)$$

In particular, if $|I| < p^{1/3}$, then

$$|I^{-1} + I^{-1}| > |I|^{2+o(1)}.$$

The aim of the present paper is to establish new additive properties of the set I^{-1}. We then combine our results with recent estimates of multilinear exponential sum bounds from [6] and obtain new results on multilinear Kloosterman sums.

The structure of the paper is as follows. In section 2 we state our results on additive properties of the set I^{-1} and on estimates of Kloosterman sums. In section 3 we give some basic preliminaries which are used throughout the paper. In sections 4–8 we give some backgrounds and prove preliminary lemmas. The proof of our results on additive properties of reciprocals on intervals (Theorems 1-6) is given in section 9. The proof of Theorems 7-13 are given in section 10. In section 11 we give the proof of Theorem 14 on Archimedian counterpart of Karatsuba's estimate, in section 12 we give the

proof of Theorem 15 on $\pi(x)-\pi(x-y)$, Theorem 16 on a linear Kloosterman sums and Theorem 17 on Brun-Titchmarsh theorem.

In this paper we consider only the case of prime modulus. The case of composite modulus will be considered in a forthcoming paper.

2 Statement of results

2.1 Reciprocals of intervals

We recall that I denotes an arbitrary non-zero interval in $\mathbb{F}_p$. We first start with results on additive properties of I^{-1}.

Theorem 1. *For any fixed positive integer constant k the number J_{2k} of solutions of the congruence*

$$x_1^{-1}+\ldots+x_k^{-1}=x_{k+1}^{-1}+\ldots+x_{2k}^{-1}, \qquad x_1,\ldots,x_{2k}\in I,$$

satisfies

$$J_{2k}<\Big(|I|^{2k^2/(k+1)}+\frac{|I|^{2k}}{p}\Big)|I|^{o(1)}. \tag{2}$$

Recall that (2) is equivalent to saying that for any $\varepsilon>0$ there exists $c=c(k;\varepsilon)>0$ such that

$$J_{2k}<c\Big(|I|^{2k^2/(k+1)}+\frac{|I|^{2k}}{p}\Big)|I|^{\varepsilon}.$$

Corollary 1. *Let $|I|<p^{1/2}$. Then for any fixed positive integer constant k,*

$$|k(I^{-1})|>|I|^{2k/(k+1)+o(1)}.$$

We remark that for $k=3$ one can prove the bound

$$|I^{-1}+I^{-1}+I^{-1}|>|I|^{1.55+o(1)}.$$

We next consider a ternary additive congruence with I^{-1}.

Theorem 2. *Let $|I|<p^{3/46}$. Then for any element $\lambda\in\mathbb{F}_p$ with*

$$\lambda\notin I^{-1}\cup\{0\}, \tag{3}$$

the number J of solutions of the congruence

$$x^{-1} + y^{-1} + z^{-1} = \lambda, \quad x, y, z \in I,$$

satisfies

$$J < |I|^{2/3+o(1)}.$$

The restriction (3) is motivated by the possibility of $|I|^{1+o(1)}$ solutions otherwise (for instance, $z = \lambda^{-1}$ and $x + y = 0$).

From Theorem 2 it easily follows that for $|I| < p^{3/46}$, one has the bound

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{7/3+o(1)}.$$

The following statements show that for sufficiently small I one has optimal bounds.

Theorem 3. *Let $|I| < p^{1/18}$. Then the number J_6 of solutions of the congruence*

$$x_1^{-1} + x_2^{-1} + x_3^{-1} = x_4^{-1} + x_5^{-1} + x_6^{-1}, \qquad x_1, \ldots, x_6 \in I,$$

satisfies

$$J_6 < |I|^{3+o(1)}.$$

In particular, for $|I| < p^{1/18}$ we have

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{3+o(1)}.$$

Theorem 4. *There is an absolute constant $c > 0$ such that for any fixed positive integer constant k and any interval $I \subset \mathbb{F}_p$ with $|I| < p^{c/k^2}$ the number J_{2k} of solutions of the congruence*

$$x_1^{-1} + \ldots + x_k^{-1} = x_{k+1}^{-1} + \ldots + x_{2k}^{-1}, \qquad x_1, \ldots, x_{2k} \in I,$$

satisfies

$$J_{2k} < |I|^{k+o(1)}.$$

In particular, for such intervals I we have

$$|k(I^{-1})| > |I|^{k+o(1)}.$$

Remark 1. *From the proof it is clear that in Theorem 4 one can take $c = 1/4$.*

Theorem 5. *Let $I = [1, N]$. Then the number J_{2k} of solutions of the congruence*

$$x_1^* + \ldots + x_k^* \equiv x_{k+1}^* + \ldots + x_{2k}^* \pmod p, \qquad x_1, \ldots, x_{2k} \in I,$$

satisfies

$$J_{2k} < (2k)^{90k^3} (\log N)^{4k^2} \Big(\frac{N^{2k-1}}{p} + 1 \Big) N^k.$$

We also give a version of Theorem 5, where the variables x_j are restricted to prime numbers. By $\mathcal{P}$ we denote the set of primes.

Theorem 6. *Let $I = [1, N]$. Then the number J_{2k} of solutions of the congruence*

$$x_1^* + \ldots + x_k^* \equiv x_{k+1}^* + \ldots + x_{2k}^* \pmod p, \qquad x_1, \ldots, x_{2k} \in I \cap \mathcal{P},$$

satisfies

$$J_{2k} < (2k)^k \Big(\frac{N^{2k-1}}{p} + 1 \Big) N^k.$$

2.2 Incomplete multilinear Kloosterman sums

Below we use the abbreviation $e_p(z) = e^{2\pi i z/p}$. The incomplete Kloosterman sums

$$\sum_{x=M+1}^{M+N} e_p(ax^* + bx),$$

where a and b are integers, $\gcd(a, p) = 1$, are well known in the literature, with a variety of applications. These sums are estimated by $O(p^{1/2} \log p)$ as a consequence of Weil bounds. For $M = 0$ and N very small (that is, $N = p^{o(1)}$) these sums have been estimated by Korolev [26].

The incomplete bilinear Kloosterman sums

$$S = \sum_{x_1=M_1+1}^{M_1+N_1} \sum_{x_2=M_2+1}^{M_2+N_2} \alpha_1(x_1) \alpha_2(x_2) e_p(a x_1^* x_2^*),$$

where $\alpha_i(x_i) \in \mathbb{C}$, $|\alpha_i(x_i)| \le 1$, are also well known in the literature. Observe, that if one of the parameters N_i is much larger than $p^{1/2}$, then S can easily

be estimated. For instance, if, say, $N_1^{1-c} > p^{1/2}$ for some $c > 0$, one can use the Weil bound and get

$$
\begin{aligned}
|S|^2 \le & N_1 \sum_{x_1=M_1+1}^{M_1+N_1} \Big| \sum_{x_2=M_2+1}^{M_2+N_2} \alpha_2(x_2) e_p(a x_1^* x_2^*) \Big|^2 \le \\
& N_1 \sum_{y=M_2+1}^{M_2+N_2} \sum_{z=M_2+1}^{M_2+N_2} \Big| \sum_{x_1=M_1+1}^{M_1+N_1} e_p(a x_1^*(y^* - z^*)) \Big| \ll N_1^2 N_2 + N_1 N_2^2 \sqrt{p} (\log p),
\end{aligned}
$$

which implies that

$$
|S| < \left(N_2^{-1/2} + N_1^{-c/2} \right) (N_1 N_2)^{1+o(1)}.
$$

Thus, the most nontrivial case is $N_i < p^{1/2}$. When $M_1 = M_2 = 0$ the sum S (in a more general form in fact) has been estimated by Karatsuba [24, 25] for very short ranges of N_1 and N_2, and by Bourgain [5] for arbitrary M_1, M_2 provided that $N_1 N_2 > p^{1/2+\varepsilon}$. A full explicit version of Bourgain's result has been given by Baker [2].

The incomplete n-linear Kloosterman sums

$$
\sum_{x_1=M_1+1}^{M_1+N_1} \cdots \sum_{x_n=M_n+1}^{M_n+N_n} e_p(a_1 x_1 + \ldots + a_n x_n + a_{n+1}(x_1 \ldots x_n)^*),
$$

where $a_i \in \mathbb{Z}$, $\gcd(a_{n+1}, p) = 1$, have been studied by Luo [28] and Shparlinski [30] for arbitrary n. The main tool they used are the bounds of Burgess [11] on incomplete Gauss sums.

Here, we combine our Theorems 1, 3, 4, 5 with the multilinear exponential sum bounds from [6] (see Lemma 1 below) and obtain new estimates on Kloosterman sums. In what follows, $\alpha_1(x_1), \ldots, \alpha_n(x_n)$ are arbitrary complex numbers with $|\alpha_i(x_i)| \le 1$.

Theorem 7. *For any intervals I_1, I_2 with*

$$
|I_1| > p^{1/18}, \qquad |I_2| > p^{5/12+\varepsilon}
$$

we have

$$
\max_{(a,p)=1} \Big| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(a x_1^* x_2^*) \Big| < p^{-\delta} |I_1| |I_2|
$$

for some $\delta = \delta(\varepsilon) > 0$.

Note that $|I_1||I_2| = p^{1/2-1/36+\varepsilon}$.

Remark 2. *The statement of Theorem 7 remains true for the general sum*

$$\sum_{x_1=1}^{N_1}\sum_{x_2=1}^{N_2}\alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*+bx_1x_2).$$

This can be achieved incorporating [5, Lemma A.8].

When $M_1 = M_2 = 0$, we prove the following result, expanding the range of applicability of Karatsuba's estimate [24].

Theorem 8. *Let $I_1 = [1, N_1]$, $I_2 = [1, N_2]$. Then uniformly over all positive integers k_1, k_2 and $\gcd(a,p) = 1$ we have*

$$\Big|\sum_{x_1\in I_1}\sum_{x_2\in I_2}\alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*)\Big| < (2k_1)^{\frac{45k_1^2}{k_2}}(2k_2)^{\frac{45k_2^2}{k_1}}(\log p)^{2(\frac{k_1}{k_2}+\frac{k_2}{k_1})}\times$$

$$\times\Big(\frac{N_1^{k_1-1}}{p^{1/2}}+\frac{p^{1/2}}{N^{k_1}}\Big)^{1/(2k_1k_2)}\Big(\frac{N_2^{k_2-1}}{p^{1/2}}+\frac{p^{1/2}}{N^{k_2}}\Big)^{1/(2k_1k_2)}N_1N_2.$$

Given N_1, N_2 we choose k_1, k_2 such that

$$N_1^{2(k_1-1)} < p \le N_1^{2k_1}, \qquad N_2^{2(k_2-1)} < p \le N_2^{2k_2}$$

and the bound will be nontrivial unless both N_1, N_2 are within p^{ε}-ratio of an element of $\{p^{\frac{1}{2l}}, l \in \mathbb{Z}_+\}$. Thus, we have the following

Corollary 2. *Let $I_1 = [1, N_1]$, $I_2 = [1, N_2]$, where for $i = 1$ or $i = 2$*

$$N_i \notin \bigcup_{j\ge 1}[p^{\frac{1}{2j}-\varepsilon},\, p^{\frac{1}{2j}+\varepsilon}].$$

Then

$$\max_{(a,p)=1}\Big|\sum_{x_1=1}^{N_1}\sum_{x_2=1}^{N_2}\alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*)\Big| < p^{-\delta}N_1N_2$$

for some $\delta = \delta(\varepsilon) > 0$.

Theorem 9. *Let $I_1, I_2 \subset \mathbb{F}_p$ be intervals of sizes N_1, N_2 in arbitrary position. Then*

$$\max_{(a,p)=1}\Big|\sum_{x_1\in I_1}\sum_{x_2\in I_2}\alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*)\Big| \ll$$
$$\ll p^{1/8}N_1^{3/4}N_2^{3/4}\Big(\frac{N_1^3}{p}+1\Big)^{1/16}\Big(\frac{N_2^3}{p}+1\Big)^{1/16}.$$

Some relevant to Theorem 9 results with intervals starting from the origin can be found in [2], [15], [19].

Theorem 10. *Let k_1, k_2 be positive integer constants, $I_1, I_2 \subset \mathbb{F}_p$ be intervals of sizes N_1, N_2 in arbitrary position and*

$$N_1 < p^{\frac{k_1+1}{2k_1}}, \qquad N_2 < p^{\frac{k_2+1}{2k_2}}.$$

Then

$$\max_{(a,p)=1}\Big|\sum_{x_1\in I_1}\sum_{x_2\in I_2}\alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*)\Big| <$$
$$\Big(p^{\frac{1}{2k_1k_2}}N_1^{-\frac{1}{k_2(k_1+1)}}N_2^{-\frac{1}{k_1(k_2+1)}}\Big)(N_1N_2)^{1+o(1)}.$$

We next consider multilinear Kloosterman sums.

Theorem 11. *Let $n \geq 7$ and $N^n > p^{1/3+\varepsilon}$. Then for any intervals $I_1, \ldots, I_n$ of length N we have*

$$\max_{(a,p)=1}\Big|\sum_{x_1\in I_1}\cdots\sum_{x_n\in I_n}\alpha_1(x_1)\ldots\alpha_n(x_n)e_p(ax_1^*\ldots x_n^*)\Big| < p^{-\delta}N^n$$

for some $\delta = \delta(\varepsilon, n) > 0$.

Theorem 12. *There exists an absolute constant $C > 0$ such that for any positive integer n and any intervals $I_1, \ldots, I_n$ of length N with $N > p^{C/n^2}$, we have*

$$\max_{(a,p)=1}\Big|\sum_{x_1\in I_1}\cdots\sum_{x_n\in I_n}\alpha_1(x_1)\ldots\alpha_n(x_n)e_p(ax_1^*\ldots x_n^*)\Big| < p^{-\delta}N^n$$

for some $\delta = \delta(n) > 0$.

Remark 3. *It can be proved that Theorem 12 holds with $C = 4$. This can be done using the geometry of numbers in the style of [9] to get a suitable for this version of our Theorem 4.*

Theorem 13. *Let $I_1, \dots, I_n$ be intervals in $[1, p-1]$ with*

$$|I_1| \cdots |I_n| > p^{1/2+\varepsilon}.$$

Then we have

$$\max_{(a,p)=1} \Big| \sum_{x_1 \in I_1} \dots \sum_{x_n \in I_n} \alpha_1(x_1) \dots \alpha_n(x_n) e_p(a x_1^* \dots x_n^*) \Big| < p^{-\delta} |I_1| \cdots |I_n|$$

for some $\delta = \delta(\varepsilon, n) > 0$.

There is the following 'Archimedian' counterpart of the Karatsuba estimate.

Theorem 14. *Let $\xi \in \mathbb{R}$ with $|\xi| > N_1 N_2$ and $k_1, k_2 \in \mathbb{Z}_+$. Then*

$$\Big| \sum_{\substack{n_1 \sim N_1 \\ n_2 \sim N_2}} e^{i \frac{1}{n_1} \frac{1}{n_2} \xi} \Big| < c(k_1, k_2, \varepsilon) \gamma \, (N_1 N_2)^{1+\varepsilon} \tag{4}$$

with

$$\gamma = \Big\{ \Big(\frac{|\xi|}{N_1 N_2} N_1^{-2k_1} + \frac{N_1 N_2}{|\xi|} N_1^{2(k_1-1)} \Big) \Big(\frac{|\xi|}{N_1 N_2} N_2^{-2k_2} + \frac{N_1 N_2}{|\xi|} N_2^{2(k_2-1)} \Big) \Big\}^{1/(4k_1k_2)}$$

Given $|\xi| > N_1 N_2$, choose k_1, k_2 satisfying

$$N_i^{2(k_i-1)} \le \frac{|\xi|}{N_1 N_2} < N_i^{2k_i}.$$

Then each factor in expression for γ in Theorem 14 is $O(1)$.

Exponential sums of the type (4) appear, for instance, in the proof of Theorem 13.8 in [18]

$$\pi(x) - \pi(x-y) \le (2-\delta) \frac{y}{\log y}, \quad x^\theta < y < x, \tag{5}$$

where, as usual, $\pi(z)$ is the number of primes not exceeding z and $\delta = \delta(\theta) > 0$. Here $\theta > 0$ may be small, x is sufficiently large in terms of θ. In [18] the proof of (5) is based on estimates of exponential sums of the form $\sum_{n \sim N} e(\frac{\xi}{n})$ using either Weil or Vinogradov, when θ is very small. Using Theorem 14 one gets a better estimate.

Theorem 15. *The estimate* (5) *holds with*

$$\delta < \frac{2(1-\theta)}{12(\theta^{-1}+1)(\theta^{-1}+0.5)+1-\theta} \sim \theta^2.$$

We shall apply trilinear exponential sum bounds from [6] (see Lemma 1 below) to a linear Kloosterman sums and Brun-Titchmarsh theorem.

Theorem 16. *The following bound holds:*

$$\max_{(a,p)=1}\Big|\sum_{n\le N} e_p(an^*)\Big| \ll \frac{(\log\log p)^3 \log p}{(\log N)^{3/2}}\, N,$$

where the implied constant is absolute.

It follows that if $N = p^{\varepsilon}$ with ε fixed, the saving is $O((\log\log p)^3/(\log p)^{1/2})$ and the estimate is nontrivial if $N > \exp((\log p)^{\frac{2}{3}}(\log\log p)^3)$. This improves some results of Korolev [26] in the case of prime moduli. We also refer the reader to [27] for some variants of the problem.

We remark that in [23] it is claimed that if $\varepsilon > 0$ is fixed, then for $p^{\varepsilon} < N < p^{4/7}$ one has the bound

$$\Big|\sum_{n=1}^{N} e_p(an^*)\Big| < \frac{N}{(\log N)^{1-\varepsilon}},$$

but the proof given there is in doubt.

For $(a,q) = 1$, $\pi(x;q,a)$ denotes the number of primes $p \le x, p \equiv a \pmod q$. We aim to improve the result of Friedlander-Iwaniec on $\pi(x;q,a)$ as follows:

Theorem 17. *Let $q = x^{\theta}$, where $\theta < 1$ is close to 1. Then*

$$\pi(x;q,a) < \frac{cx}{\phi(q)\log\frac{x}{q}}$$

with $c = 2 - c_1(1-\theta)^2$, for some absolute constant $c_1 > 0$ and all sufficiently large x in terms of θ.

The constant c_1 is effective and can be made explicit.

3 Preliminaries

Throughout the paper we will use well-known connections between the number of solutions of symmetric equations and the cardinality of corresponding set. Let T be the number of solutions of the equation

$$x_1 + \ldots + x_n = y_1 + \ldots + y_n,$$

where for each i the variables x_i, y_i run through a set A_i. Then for any subset

$$\Omega \subset A_1 \times \ldots \times A_n,$$

one has the bound

$$|\{x_1 + \ldots + x_n : \ (x_1, \ldots x_n) \in \Omega\}| \geq \frac{|\Omega|^2}{T}.$$

This estimate follows from the observation that if $T_n(\Omega; \lambda)$ is the number of solutions of the equation

$$x_1 + \ldots + x_n = \lambda, \quad (x_1, \ldots, x_n) \in \Omega,$$

and

$$X = \{x_1 + \ldots + x_n : \ (x_1, \ldots x_n) \in \Omega\},$$

then

$$T \geq \sum_{\lambda \in X} T_n(\Omega; \lambda)^2 \geq \frac{1}{|X|}\Big|\sum_{\lambda \in X} T_n(\Omega; \lambda)\Big|^2 = \frac{|\Omega|^2}{|X|}.$$

In particular,

$$|A_1 + \ldots + A_n| = \#\{a_1 + \ldots + a_n : \ a_i \in A_i\} \geq \frac{|A_1|^2 \ldots |A_n|^2}{T}.$$

We note that if $A_1, \ldots, A_{2n} \subset \mathbb{F}_p$ and $T_{2n}(\lambda)$ is the number of solutions of the congruence

$$x_1 + \ldots + x_{2n} \equiv \lambda \pmod p, \quad (x_1, \ldots, x_{2n}) \in A_1 \times \ldots \times A_{2n},$$

then

$$T_{2n}(\lambda) \leq (J_1 \ldots J_{2n})^{\frac{1}{2n}},$$

where J_i is the number of solutions of the congruence

$$y_1 + \ldots + y_n \equiv y_{k+1} + \ldots + y_{2k} \pmod p, \qquad y_1, \ldots, y_{2k} \in A_i.$$

Indeed, we have

$$T = \frac{1}{p}\sum_{a=0}^{p-1}\sum_{x_1\in A_1}\ldots\sum_{x_{2n}\in A_{2n}} e_p(ax_1)\ldots e_p(ax_{2n})e_p(-a\lambda).$$

Applying Hölder's inequality we get

$$T \leq \prod_{j=1}^{n}\Big(\frac{1}{p}\sum_{a=0}^{p-1}\Big|\sum_{x_j\in A_j} e_p(ax_j)\Big|^{2n}\Big)^{\frac{1}{2n}} = (J_1\ldots J_{2n})^{\frac{1}{2n}}.$$

In proofs of some of our results we will use the observation that if $X, Y \in \mathbb{F}_p$, then the number of solutions of the congruence equation

$$\frac{1}{y+x_1} + \ldots + \frac{1}{y+x_n} = \frac{1}{y+x_{n+1}} + \ldots + \frac{1}{y+x_{2n}}, \quad x_i \in X,\ y \in Y,$$

is at most $O(|X|^nY + |X|^{2n})$, the implied constant may depend only on n. Indeed, the contribution from those $(x_1, \ldots, x_{2n}) \in X^{2n}$ for which the series $x_1, \ldots, x_{2n}$ contains at most n distinct elements, is $O(|X|^n|Y|)$. On the other hand, if there are more than n distinct elements in this series, then we can assume that $x_1 \notin \{x_2, \ldots, x_{2n}\}$. For each such given $(x_1, \ldots, x_{2n}) \in X^{2n}$ the polynomial

$$P(Z) = \prod_{i\neq 1}(Z+x_i) + \ldots + \prod_{i\neq n}(Z+x_i) - \prod_{i\neq n+1}(Z+x_i) - \ldots - \prod_{i\neq 2n}(Z+x_i)$$

is nonzero (as $P(-x_1) \neq 0$) and since $P(y) = 0$ we get at most $2n-1$ possibilities for y. See also [2, Lemmas 2,3] for more general statements.

4 Multilinear exponential sums

The following result, which we state as a lemma, has been proved by Bourgain [6]. It is based on results from additive combinatorics, in particular sum-product estimates. This lemma will be used in the proof of our results on Kloosterman sums.

Lemma 1. *Let $\gamma_1(x_1), \dots, \gamma_n(x_n)$ be non-negative real numbers satisfying*

$$\|\gamma_i\|_1 = \sum_{x=0}^{p-1} |\gamma_i(x)| \le 1, \quad \|\gamma_i\|_2 = \Big(\sum_{x=0}^{p-1} |\gamma_i(x)|^2\Big)^{1/2} < p^{-\delta}.$$

Assume further

$$\prod_{i=1}^{n} \|\gamma_i\|_2 < p^{-1/2-\delta},$$

where $0 < \delta < 1/4$. Then there is the exponential sum bound

$$\Big|\sum_{x_1=0}^{p-1} \dots \sum_{x_n=0}^{p-1} \gamma_1(x_1) \dots \gamma_n(x_n) e_p(x_1 \dots x_n)\Big| < p^{-\delta'}$$

with some $\delta' > (\delta/n)^{Cn}$.

5 Resultant Bound

We shall need the following resultant bound from [9].

Lemma 2. *Let $N \ge 1$, $\sigma, \vartheta \in \mathbb{R}$, and let $m, n \ge 2$ be fixed integers. Assume also that one of the following conditions hold:*

(i) $\sigma \ge 0$;

(ii) $\vartheta \ge 0$;

(iii) $\sigma + \vartheta \ge -1$.

Let $P_1(Z)$ and $P_2(Z)$ be non-constant polynomials with integer coefficients,

$$P_1(Z) = \sum_{i=0}^{m-1} a_i Z^{m-1-i}, \qquad P_2(Z) = \sum_{i=0}^{n-1} b_i Z^{n-1-i}$$

such that

$$\begin{aligned} |a_i| &< AN^{i+\sigma}, \quad i = 0, \dots, m-1, \\ |b_i| &< AN^{i+\vartheta}, \quad i = 0, \dots, n-1, \end{aligned}$$

for some A. Then

$$\mathrm{Res}(P_1, P_2) \ll N^{(m-1+\sigma)(n-1+\vartheta)-\sigma\vartheta.},$$

where the implicit constant in $\ll$ depends only on A, m and n.

6 Background on geometry of numbers

We need some facts from the geometry of numbers. Recall that a lattice in $\mathbb{R}^n$ is an additive subgroup of $\mathbb{R}^n$ generated by n linearly independent vectors. Take an arbitrary convex compact and symmetric with respect to 0 body $D \subset \mathbb{R}^n$. Recall that, for a lattice $\Gamma \subset \mathbb{R}^n$ and $i = 1, \ldots, n$, the i-th successive minimum $\lambda_i(D, \Gamma)$ of the set D with respect to the lattice Γ is defined as the minimal number λ such that the set λD contains i linearly independent vectors of the lattice Γ. Obviously, $\lambda_1(D, \Gamma) \le \ldots \le \lambda_n(D, \Gamma)$. We need the following result given in [3, Proposition 2.1] (see also [31, Exercise 3.5.6] for a simplified form that is still enough for our purposes).

Lemma 3. *We have*

$$|D \cap \Gamma| \le \prod_{i=1}^{n} \left(\frac{2i}{\lambda_i(D, \Gamma)} + 1 \right).$$

Denoting, as usual, by $(2n+1)!!$ the product of all odd positive numbers up to $2n+1$, we get the following

Corollary 3. *We have*

$$\prod_{i=1}^{n} \min\{\lambda_i(D, \Gamma), 1\} \le \frac{(2n+1)!!}{|D \cap \Gamma|}.$$

7 Equations with many variables

The following lemma is due to Karatsuba [24].

Lemma 4. *The following bound holds:*

$$\left| \left\{ (x_1, \ldots, x_{2k}) \in [1, N]^{2k} : \quad \frac{1}{x_1} + \ldots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \ldots + \frac{1}{x_{2k}} \right\} \right| < (2k)^{80k^3} (\log N)^{4k^2} N^k.$$

The following elementary statement will be used to exclude some degenerated cases in the proof of Lemma 6 below.

Lemma 5. *Let $c \in \mathbb{C}$, $c_1, \ldots, c_r \in \mathbb{C}^*$, S be a finite subset of $\mathbb{C}$. Let T_r be the number of solutions of the equation*

$$c_1x_1 + \ldots + c_rx_r = c, \qquad x_1, \ldots, x_r \in S,$$

and J_{2s} be the number of solutions of the equation

$$x_1 + \ldots + x_s = x_{s+1} + \ldots + x_{2s}, \qquad x_1, \ldots, x_{2s} \in S.$$

If $r = 2k$ for some integer k, then $T_{2k} \leq J_{2k}$. If $r = 2k - 1$ for some integer k, then $T_{2k-1}^2 \leq J_{2k-2}J_{2k}$.

Proof. Let $r = 2k$. Among all $2k+1$-tuples $(l_1, \ldots, l_{2k}, l)$ with

$$l_i \in \{\pm c_1, \ldots, \pm c_{2k}\}, \quad l \in \{0, c\}$$

we consider the one for which the number of solutions of the equation

$$l_1x_1 + \ldots + l_{2k}x_{2k} = l, \qquad x_1, \ldots, x_{2k} \in S, \tag{6}$$

is maximal. There can be several $2k+1$-tuples with this property. We choose the one for which the sequence

$$l_1, \ldots, l_{2k}$$

contains the maximal number of elements from $\{-l_1, l_1\}$. We fix one such $(l_1, \ldots, l_{2k}, l)$ with

$$l_i \in \{-l_1, l_1\}, \quad i = 1, \ldots, s,$$

such that either $s = 2k$ or $l_t \notin \{-l_1, l_1\}$ for $t > s$. Denote by L_{2k} the number of solutions of (6), that is

$$l_1x_1 + \ldots + l_kx_k = l - (l_{k+1}x_{k+1} + \ldots + l_{2k}x_{2k}); \qquad x_1, \ldots, x_{2k} \in S.$$

Note that

$$L_{2k} = \sum_{\lambda} I_1(\lambda)I_2(\lambda),$$

where $I_1(\lambda)$ is the number of solutions of the equation

$$l_1x_1 + \ldots + l_kx_k = \lambda, \qquad x_1, \ldots, x_k \in S,$$

and $I_2(\lambda)$ is the number of solutions of the equation

$$l - (l_{k+1}x_{k+1} + \ldots + l_{2k}x_{2k}) = \lambda; \quad x_{k+1}, \ldots, x_{2k} \in S.$$

Applying the Cauchy-Schwarz inequality, we obtain

$$L_{2k}^2 \leq \Big(\sum_{\lambda} I_1^2(\lambda)\Big)\Big(\sum_{\lambda} I_2^2(\lambda)\Big).$$

The quantity in the second parenthesis is equal to the number of solutions of the equation

$$l_{k+1}x_1 + \ldots + l_k x_k = l_{k+1}x_{k+1} + \ldots + l_{2k}x_{2k}, \qquad x_1, \ldots, x_{2k} \in S.$$

Hence, by the maximality of L_{2k} we have

$$L_{2k} \leq \sum_{\lambda} I_1^2(\lambda).$$

The right hand side indicates the number of solutions of the equation

$$l_1x_1 + \ldots + l_k x_k = l_1 x_{k+1} + \ldots + l_k x_{2k}, \qquad x_1, \ldots, x_{2k} \in S. \tag{7}$$

Clearly, the series

$$l_1, \ldots, l_k, l_1, \ldots, l_k$$

contains $\min\{2s, 2k\}$ elements from $\{-l_1, l_1\}$. Hence, by the maximality of s we have $s = 2k$. Therefore, $l_i \in \{-l_1, l_1\}$ for all i, which implies that the number of solutions of the equation (7) is equal to J_{2k}. Thus, $L_{2k} \leq J_{2k}$ implying $T_{2k} \leq I_{2k}$. This proves the first statement of the lemma.

To prove the second statement of our lemma, we write the corresponding to T_{2k-1} equation in the form

$$c_1x_1 + \ldots + c_k x_k = l - (c_{k+1}x_{k+1} + \ldots + c_{2k-1}x_{2k-1})$$

and, as before, apply the Cauchy-Schwarz inequality to get that

$$T_{2k-1}^2 \leq \Big(\sum_{\lambda} I_{11}^2(\lambda)\Big)\Big(\sum_{\lambda} I_{22}^2(\lambda)\Big),$$

where $I_{11}(\lambda)$ is the number of solutions of the equation

$$c_1x_1 + \ldots + c_k x_k = \lambda, \qquad x_1, \ldots, x_k \in S$$

and $I_{22}(\lambda)$ is the number of solutions of the equation

$$-(c_{k+1}x_{k+1} + \ldots + c_{2k-1}x_{2k-1}) = \lambda, \qquad x_{k+1}, \ldots, x_{2k-1} \in S.$$

Applying the first statement of our lemma we obtain

$$\sum_{\lambda} I_{11}^2(\lambda) \le J_{2k}; \quad \sum_{\lambda} I_{22}^2(\lambda) \le J_{2k-2},$$

which finishes the proof of the lemma. $\square$

Let ξ be an algebraic integer of degree d and $O_{\mathbb{K}}$ be the ring of integers in $\mathbb{K} = \mathbb{Q}(\xi)$. In the proof of Lemma 6 below we use the language of ideals in the Dedekind domain $O_{\mathbb{K}}$. We refer the reader to [22, Chapter 12] and [4, Chapter 3] for a background material. Below, all considered ideals are integral. In particular, we say that an ideal I_2 divides I_1 if for some ideal I_3 we have $I_1 = I_2 I_3$.

We will use well-known properties of ideals. For instance, if I_1 and I_2 are ideals such that $I_1 \subset I_2$ then I_2 divides I_1 (see, for example, [22, Proposition 12.2.7]).

Clearly, the uniqueness of factorization into prime ideals implies that if I_1, I_2, I_3 are ideals in $O_{\mathbb{K}}$ such that I_3 divides $I_1 I_2$ then $I_3 = J_1 J_2$ for some ideals J_1 dividing I_1 and J_2 dividing I_2, respectively.

It is also useful to recall that the number of integral ideals in $O_{\mathbb{K}}$ of norm n is at most $\tau(n)^d$, where τ is the divisor function. In particular, for fixed constant d and large n this is a quantity of size $n^{o(1)}$.

We recall that the logarithmic height of a nonzero polynomial $P \in \mathbb{Z}[Z]$ is defined as the maximum logarithm of the largest (by absolute value) coefficient of P. The logarithmic height of an algebraic number α is defined as the logarithmic height of its minimal polynomial. It is a well-known consequence of basic properties of Mahler's measure that if $P, Q \in \mathbb{Z}[Z]$ are two univariate non-zero polynomials with $Q \mid P$ and if P is of logarithmic height at most H then Q is of logarithmic height at most $H + O(1)$, where the implied constant depends only on $\deg P$ (see, for example, [29, Theorem 4.2.2]).

In particular, it follows that if $P \in \mathbb{Z}[Z]$ is a nonconstant polynomial with coefficients bounded by M (by absolute value), then every root σ of $P(Z)$ can be represented in the form ξ/q where ξ is an algebraic integer of logarithmic height at most $O(\log M)$ and $q > 0$ is an integer with $q < M^{O(1)}$, where the implied constants depend only on $\deg P$.

Lemma 6. *For any fixed positive integer constant r and all values of $\sigma \in \mathbb{C}$ the number $T_r(\sigma, N)$ of solutions of the equation*

$$\frac{1}{\sigma + x_1} + \ldots + \frac{1}{\sigma + x_r} = \frac{1}{\sigma + x_{r+1}} + \ldots + \frac{1}{\sigma + x_{2r}}$$

in positive integers $x_1, \ldots, x_{2r} \le N$ satisfies

$$T_r(a, N) < N^{r+o(1)}.$$

Proof. For the brevity denote $T_r = T_r(a, N)$. We shall prove the lemma by induction on r. For $r = 1$ the result is trivial. Let $r \ge 2$.

From Lemma 5 it follows that the number of solutions satisfying $x_i = x_j$ for some $i \ne j$ contributes to T_r a quantity bounded by

$$O(\sqrt{T_{r-1}T_r})$$

Thus, by the induction hypothesis it suffices to prove that

$$T_r' < N^{r+o(1)},$$

where T_r' denotes the number of solutions with $x_i \ne x_j$ for all $i \ne j$. We can assume that $T_r' > N^r$ as otherwise there is nothing to prove. Rewrite our equation in the form

$$\prod_{i\ne 1}(\sigma + x_i) + \ldots + \prod_{i \ne r}(\sigma + x_i) = \prod_{i\ne r+1}(\sigma + x_i) + \ldots + \prod_{i\ne 2r}(\sigma + x_i)$$

and consider the polynomial $P(Z)$ defined as

$$\prod_{i\ne 1}(Z + x_i) + \ldots + \prod_{i \ne r}(Z + x_i) - \prod_{i\ne r+1}(Z + x_i) - \ldots - \prod_{i\ne 2r}(Z + x_i).$$

Clearly, $\deg P \le 2r - 1$. Note also that $P(-x_1) \ne 0$, so $P(Z)$ is not a zero polynomial. Moreover, $P(\sigma) = 0$, implying that $P(Z)$ is not a constant polynomial either. Therefore, we may assume that σ is an algebraic number of degree d with $1 \le d \le 2r - 1$ and logarithmic height $O(\log N)$. We can write $\sigma = \xi/q$, where ξ is an algebraic integer of height $O(\log N)$ and q is an integer with $q = N^{O(1)}$. Then our equation takes the form

$$\prod_{i\ne 1}(\xi + qx_i) + \ldots + \prod_{i \ne r}(\xi + qx_i) = \prod_{i\ne r+1}(\xi + qx_i) + \ldots + \prod_{i\ne 2r}(\xi + qx_i). \quad (8)$$

Let $O_{\mathbb{K}}$ be the ring of integers in $\mathbb{K} = \mathbb{Q}(\xi)$. The idea is to use the observation that for each $i = 1, \ldots, 2r$

$$\xi + qx_i \quad \text{divides} \quad q^{2r-1} \prod_{j \neq i} (x_j - x_i). \tag{9}$$

The strategy to evaluate the number of solutions of (8) is to introduce consequently the variables $x_1, x_2, \ldots$ taking into account congruence conditions that appeared fixing previous variables.

Given an ideal I we denote by $\nu(I)$ its norm. We factor the principal ideal $(\xi + qx_1)$ into factors

$$(\xi + qx_1) = I_1 J_1,$$

where the prime factors of I_1 divide q and $(J_1, q) = 1$. By (9), the norm $\nu(J_1)$ divides $\prod\limits_{j \geq 2} (x_j - x_1)^d$. Hence,

$$x_j \equiv x_1 \pmod{r_j}, \quad 2 \leq j \leq 2r, \tag{10}$$

for some $r_j \in \mathbb{Z}_+$ such that $\nu(J_1) \mid \nu_1^d$ with $\nu_1 = \prod\limits_{j \geq 2} r_j$ and $\nu_1 \mid \nu(J_1)$. We restrict ν_1 to dyadic intervals, that is there exists a fixed number $\mu_1 \geq 1$ such that if we restrict ν_1 to the size range

$$\mu_1 \leq \nu_1 \leq 2\mu_1, \tag{11}$$

then the number of solutions of our equation with this restriction will be changed by at most $N^{o(1)}$ times.

For every x_1 we consider at most $N^{o(1)}$ different cases and in accordance to (10) specify x_j, $j \geq 2$, to arithmetic progressions $L_{2,j} \in [1, N]$, where thus

$$\prod_{j \geq 2} |L_{2,j}| < \frac{N^{2r-1+o(1)}}{\mu_1}. \tag{12}$$

At the next step for $x_2 \in L_{2,2}$ we factor

$$(\xi + qx_2) = I_2 J_2,$$

where the prime factors of I_2 divide q or $\nu(\xi + qx_1)$ and J_2 is coprime to q and $\nu(\xi + qx_1)$. Hence, J_2 is coprime to $(x_2 - x_1)$ and again by (9), the norm

$\nu(J_2)$ divides $\prod_{j\geq 3}(x_j - x_2)^d$. Arguing as before, we find ν_2 such that $\nu(J_2) \mid \nu_2^d$ and $\nu_2 \mid \nu(J_2)$. We can restrict ν_2 to a size range, that is there exists a fixed number $\mu_2 \geq 1$ (independent on variables x_i) such that if we restrict ν_2 to

$$\mu_2 \leq \nu_2 \leq 2\mu_2, \tag{13}$$

then the number of solutions of our equation with this restriction will be changed by at most $N^{o(1)}$ times. For every $x_2 \in L_{2,2}$ we can consider at most $N^{o(1)}$ possibilities and specify x_j, $j \geq 3$, to arithmetic progressions $L_{3,j} \subset L_{2,j}$ where

$$\prod_{j\geq 3}|L_{3,j}| \leq \frac{1}{\mu_2}\prod_{j\geq 3}|L_{2,j}|, \qquad \nu(J_2) \mid \nu_2^d. \tag{14}$$

Note indeed that the progression $L_{2,j}$ are defined to some modulus $r_j \mid \nu_1$ and $\gcd(r_j, \nu(J_2)) = 1$ since $\nu(J_1)$, $\nu(J_2)$ are coprime.

At the next step for $x_3 \in L_{3,3}$ we factor

$$(\xi + qx_3) = I_3 J_3,$$

where the prime factors of I_3 divides either $(q), \nu(\xi + qx_1)$ or $\nu(\xi + qx_2)$, and J_3 is coprime with $(q), \nu(\xi + qx_1)$ and $\nu(\xi + qx_2)$. We find ν_3 similar to the previous cases and specify it to a size range $\mu_3 \leq \nu_3 \leq 2\mu_3$, where μ_3 is independent on variables. The continuation of the process is clear.

We now consequently fix $x_1 \leq N$, $x_2 \in L_{2,2}, \ldots, x_{2r} \in L_{2r,2r}$, that is, we fix x_1 and considering $N^{o(1)}$ possibilities for arithmetic progressions $L_{2,j}, j \geq 3$, we fix $x_2 \in L_{2,2}$, then considering $N^{o(1)}$ possibilities for arithmetic progressions $L_{3,j}, j \geq 3$, we fix $x_3 \in L_{3,3}$ and iterate this until we fix $x_{2r} \in L_{2r,2r}$. We estimate the number of solutions of (8) as $N^{o(1)}$ contributions of the form

$$N|L_{2,2}||L_{3,3}|\ldots|L_{2r,2r}|.$$

From (12), (14) and iteration we get

$$\begin{aligned} N^{2r-1} &\gtrapprox \mu_1|L_{2,2}|\prod_{j\geq 3}|L_{2,j}| \\ &\gtrapprox \mu_1\mu_2|L_{2,2}||L_{3,3}|\prod_{j\geq 4}|L_{3,j}| \\ &\qquad\ldots \\ &\gtrapprox \mu_1\ldots\mu_{2r-1}|L_{2,2}|\ldots|L_{2r,2r}|. \end{aligned}$$

Here $A \gtrapprox B$ means $A > BN^{o(1)}$. Thus, the number of solutions of (8) may be bounded by

$$\frac{N^{2r+o(1)}}{\mu_1 \dots \mu_{2r-1}}. \tag{15}$$

Next, returning to our construction, it is clear that $\nu(I_1) = N^{O(1)}$ and since the prime factors of I_1 divide q, it follows that the number of possibilities for I_1 is at most $N^{o(1)}$. Fixing I_1 and denoting $\xi_1 = \xi, \xi_2, \dots, \xi_d$ the conjugates of ξ, we have

$$\prod_{s=1}^{d} (\xi_s + qx_1) = \nu(I_1)\nu(J_1)$$

and since $\nu(J_1) \mid \nu_1^d$ it follows that $\nu(J_1)$ is determined by ν_1 with up to $N^{o(1)}$ possibilities. Thus, given ν_1 we retrieve x_1 with up to $N^{o(1)}$ possibilities. It follows that in the size range (11) the number of possibilities for x_1 is at most $N^{o(1)}\mu_1$. Next, once x_1 is given, there are at most $N^{o(1)}$ possibilities for the ideal I_2 and similarly $N^{o(1)}\mu_2$ possibilities for x_2. It follows that the number of possibilities for $x_1, x_2, \dots, x_{2r-1}$ is at most $\mu_1\mu_2 \dots \mu_{2r-1}N^{o(1)}$. Thus, the number of solutions of (8) is bounded by $\mu_1\mu_2 \dots \mu_{2r-1}N^{o(1)}$. Since it is also bounded by (15), the result follows. ☐

Lemma 7. *Let $x, y, z, a_1, a_2, b_1, b_2$ be complex numbers such that*

$$\begin{cases} xyz = a_1(x+y+z) + b_1, \\ xy + yz + zx = a_2(x+y+z) + b_2, \end{cases}$$

Then

$$(x^2 - a_2x + a_1)(y^2 - a_2y + a_1)(z^2 - a_2z + a_1) = (b_1 - \alpha_1 b_2 - \alpha_1^3)(b_1 - \alpha_2 b_2 - \alpha_2^3),$$

where

$$\alpha_1 = \frac{a_2 + \sqrt{a_2^2 - 4a_1}}{2}, \quad \alpha_2 = \frac{a_2 - \sqrt{a_2^2 - 4a_1}}{2}.$$

Proof. Indeed, since $\alpha_i^2 - a_2\alpha_i + a_1 = 0$, we have

$$(x - \alpha_i)(y - \alpha_i)(z - \alpha_i) = b_1 - \alpha_i b_2 - \alpha_i^3, \quad i = 1, 2.$$

Multiplying these equalities the claim follows. ☐

Lemma 8. *Let A, B be integers with $AB \neq 0$ and $|A|, |B| < N^{O(1)}$. Then the diophantine equation*

$$Axy + Bx + By = 0 \tag{16}$$

has at most $N^{o(1)}$ solutions in integers x, y with $|x|, |y| \leq N^{O(1)}$.

Proof. Indeed, we have

$$(Ax + B)(Ay + B) = B^2$$

and the statement follows from the well-known bound for the divisor function. $\square$

Lemma 9. *Let a_0, b_0, u_0, v_0 be integers with $b_0 u_0 v_0 \neq 0$ and*

$$|a_0|, |b_0|, |u_0|, |v_0| < N^{O(1)}.$$

Assume that

$$\frac{u_0}{v_0} \notin \Big\{ \frac{b_0}{a_0 + b_0 x} : \quad 1 \leq x \leq N \Big\}.$$

Then the number J of solutions of the diophantine equation

$$u_0(a_0 + b_0x_1)(a_0 + b_0x_2)(a_0 + b_0x_3) = v_0 b_0 \times$$
$$\Big((a_0 + b_0x_1)(a_0 + b_0x_2) + (a_0 + b_0x_2)(a_0 + b_0x_3) + (a_0 + b_0x_3)(a_0 + b_0x_1) \Big)$$

in integers x_1, x_2, x_3 with

$$1 \leq x_i \leq N, \quad a_0 + b_0 x_i \neq 0,$$

satisfies

$$J < N^{2/3 + o(1)}.$$

Proof. We can clearly assume that

$$b_0 > 0, \quad v_0 > 0, \quad \gcd(a_0, b_0) = 1.$$

We observe that if one of the variables x_1, x_2, x_3 is determined, then for the rest two variables there remain at most $N^{o(1)}$ possibilities. Indeed, let x_1 be fixed. Then denoting

$$X_i = a_0 + b_0 x_i, \quad A = u_0 X_1 - v_0 b_0, \quad B = -v_0 b_0 X_1,$$

we get

$$AX_2X_3 + BX_2 + BX_3 = 0.$$

By the condition, $AB \neq 0$ and $|A|, |B| < N^{O(1)}$. Hence by Lemma 8, we can retrieve X_2, X_3, and thus the numbers x_2, x_3, with at most $N^{o(1)}$ possibilities.

Denote

$$u_0' = \frac{u_0}{\gcd(u_0, b_0v_0)}, \qquad \frac{b_0v_0}{\gcd(u_0, b_0v_0)} = w_0 \geq 1.$$

We have

$$u_0'(a_0 + b_0x_1)(a_0 + b_0x_2)(a_0 + b_0x_3) = w_0 \times$$
$$\Big((a_0 + b_0x_1)(a_0 + b_0x_2) + (a_0 + b_0x_2)(a_0 + b_0x_3) + (a_0 + b_0x_3)(a_0 + b_0x_1)\Big)$$

Since $(u_0', w_0) = 1$, there exists a representation

$$w_0 = w_1w_2w_3 \tag{17}$$

and non-zero integers y_1, y_2, y_3 such that

$$a_0 + b_0x_i = w_iy_i, \quad i = 1, 2, 3. \tag{18}$$

In particular,

$$u_0'y_1y_2y_3 = w_1w_2y_1y_2 + w_2w_3y_2y_3 + w_3w_1y_3y_1. \tag{19}$$

We can assume that

$$w_1 \geq w_2 \geq w_3 \geq 1.$$

By the bound for the divisor function, the representation (17) implies that there are at most $N^{o(1)}$ possible values for w_1, w_2, w_3. Let us fix one such representation. Having w_1, w_2, w_3 fixed, we observe that the condition $\gcd(a_0, b_0) = 1$ and the equality

$$a_0 + b_0x_1 = w_1y_1 \tag{20}$$

imply that $\gcd(b_0, w_1) = 1$. Hence, (20) uniquely determines $x_1 \pmod{w_1}$. It then follows that there are at most

$$N^{1+o(1)}w_1^{-1} + 1$$

possible values for x_1. Then we retrieve x_2, x_3 and get the bound

$$J < N^{1+o(1)}w_1^{-1} + N^{o(1)}. \tag{21}$$

Next, from (19) and $w_1 \geq w_2 \geq w_3 \geq 1$ we have

$$|u_0'| \min\{|y_1|, |y_2|, |y_3|\} \leq 3w_1^2.$$

Thus,

$$\min\{|y_1|, |y_2|, |y_3|\} \leq 3w_1^2.$$

Hence, we can determine one of y_1, y_2, y_3 with $O(w_1^2)$ possibilities. Consequently, by (18) we determine one of x_1, x_2, x_3 and thus we get

$$J < w_1^2 N^{o(1)}.$$

Comparing this with (21), we conclude $J < N^{2/3+o(1)}$.

$\square$

8 Congruences

In what follows, N is a large parameter, $N < p$. We start with the following result from [12] which is based on the idea of Heath-Brown [20].

Lemma 10. *Let $\lambda \not\equiv 0 \pmod p$. Then the number J of solutions of the congruence*

$$xy \equiv \lambda \pmod p, \qquad L+1 \leq x, y \leq L+N,$$

satisfies

$$J < \frac{N^{3/2+o(1)}}{p^{1/2}} + N^{o(1)}.$$

In particular, if $N < p^{1/3}$, then one has $J < N^{o(1)}$.

Corollary 4. *Let $\lambda \not\equiv 0 \pmod p$. Then the number J of solutions of the congruence*

$$\frac{1}{x} + \frac{1}{y} \equiv \lambda \pmod p, \qquad L+1 \leq x, y \leq L+N,$$

satisfies

$$J < \frac{N^{3/2+o(1)}}{p^{1/2}} + N^{o(1)}.$$

In particular, if $N < p^{1/3}$, then one has $J < N^{o(1)}$.

Proof. Indeed, we have

$$(x-\lambda^{-1})(y-\lambda^{-1}) \equiv \lambda^{-2} \pmod p$$

and the claim follows from Lemma 10. $\square$

The following result has been proved in [12] (see also [8] for the extension of [12] to higher dimensional case).

Lemma 11. *Let* $\lambda \not\equiv 0 \pmod p$ *and* $N < p^{1/8}$. *Then the number* J *of solutions of the congruence*

$$xyz \equiv \lambda \pmod p, \qquad L+1 \le x, y \le L+N,$$

satisfies

$$J < N^{o(1)}.$$

The following lemma follows from the work of Ayyad, Cochrane and Zheng [1] (and from Lemma 10 when $|I_1||I_2|$ is very small). In fact, we shall only apply this lemma when one of the intervals starts from the origin, the result which had previously been established by Friedlander and Iwaniec [16].

Lemma 12. *Let* I_1, I_2 *be two intervals in* $\mathbb{F}_p^*$ *with*

$$|I_1||I_2| < p.$$

Then the number of solutions of the congruence

$$xy = zt, \quad (x,z) \in I_1 \times I_1, \quad (y,t) \in I_2 \times I_2,$$

is not greater than $(|I_1||I_2|)^{1+o(1)}$.

The following lemma will be used in the proof of Theorems 2 and 3. It is given with explicit constants to make the statement more transparent, the reader should not take them seriously.

Lemma 13. *Let* $I = \{a+1, \ldots, a+N\}$ *and*

$$\lambda \not\equiv 0 \pmod p, \quad \lambda \notin \{x^{-1} \pmod p : \quad x \in I\}.$$

Assume that

$$|I| = N < 0.1 p^{1/18} J^{2/9}$$

where J is the number of solutions of the congruence

$$x^{-1} + y^{-1} + z^{-1} \equiv \lambda \pmod p, \quad x, y, z \in I.$$

Let also $J > N^{\varepsilon}$ for some fixed small constant $\varepsilon > 0$ and let N be sufficiently large. Then there exist integers $\Delta_4', \Delta_4'', \Delta_3$ with

$$|\Delta_4'| < 10^5 N^4/J, \quad |\Delta_4''| < 10^5 N^4/J, \quad |\Delta_3| < 10^5 N^3/J$$

such that

$$a \equiv \frac{\Delta_4'}{\Delta_3} \pmod p; \quad \lambda^{-1} \equiv \frac{\Delta_4''}{\Delta_3} \pmod p.$$

Proof. It follows that J is the number of solutions of the congruence

$$\begin{aligned}&\lambda(a+x)(a+y)(a+z)\\ &\qquad \equiv (a+x)(a+y) + (a+y)(a+z) + (a+z)(a+x) \pmod p\end{aligned}$$

in positive integers $x, y, z \le N$ with $(a+x)(a+y)(a+z) \not\equiv 0 \pmod p$.

Note that by Corollary 4 we have $J < N^{1+o(1)}$ so that $N < p^{1/13}$. We rewrite the congruence in the form

$$\begin{aligned}&xyz + (a-\lambda^{-1})(xy+yz+zx)+\\ &\quad (a^2 - 2a\lambda^{-1})(x+y+z) + (a^3 - 3a^2\lambda^{-1}) \equiv 0 \pmod p.\end{aligned} \tag{22}$$

We fix one solution (x_0, y_0, z_0) and get

$$\begin{aligned}&(a^2 - 2a\lambda^{-1})(x+y+z-A_0)\\ &\quad +(a-\lambda^{-1})(xy+yz+zx-B_0) + (xyz - C_0) \equiv 0 \pmod p.\end{aligned} \tag{23}$$

where

$$A_0 = x_0 + y_0 + z_0, \quad B_0 = x_0y_0 + y_0z_0 + z_0x_0, \quad C_0 = x_0y_0z_0$$

We use some ideas from [9]. Define the lattice

$$\Gamma = \{(u, v, w) \in \mathbb{Z}^3 \ : \ (a^2 - 2a\lambda^{-1})u + (a - \lambda^{-1})v + w \equiv 0 \pmod p\}$$

and the body

$$D = \{(u, v, w) \in \mathbb{R}^3 \ : \ |u| \le 3N, \ |v| \le 3N^2, \ |w| \le N^3\}.$$

Since any given vector

$$(x+y+z-A_0, xy+yz+zx-B_0, xyz-C_0)$$

defines the values of x, y, z with at most 6 possibilities, we have

$$|D \cap \Gamma| \geq J/6.$$

Therefore, by Corollary 3, the successive minimas $\lambda_i = \lambda_i(D, \Gamma)$, $i = 1, 2, 3$, satisfy the inequality

$$\prod_{i=1}^{3} \min\{1, \lambda_i\} < 1000 J^{-1}.$$

In particular, we have $\lambda_1 \leq 1$. By the definition of λ_i, there are linearly independent vectors

$$(u_i, v_i, w_i) \in \lambda_i D \cap \Gamma, \qquad i = 1, 2, 3.$$

We consider separately the following three cases.

Case 1: $\lambda_3 \leq 1$. Thus, we have $\lambda_1\lambda_2\lambda_3 < 1000 J^{-1}$. We consider the determinant

$$\Delta = \det \begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}.$$

Clearly,

$$|\Delta| < 6N^6 \lambda_1\lambda_2\lambda_3 < 6000 N^6/J < p.$$

Thus, $|\Delta| < p$. On the other hand, from

$$(a^2 - 2a\lambda^{-1})u_i + (a - \lambda^{-1})v_i + w_i \equiv 0 \pmod{p}, \qquad i = 1, 2, 3,$$

we conclude that Δ is divisible by p. Therefore, $\Delta = 0$, which contradicts the linear independence of the vectors (u_i, v_i, w_i), $i = 1, 2, 3$. Thus, this case is impossible.

Case 2: $\lambda_1 \leq 1, \lambda_2 > 1$. Since $\lambda_2 > 1$ we see that

$$(x+y+z-A_0, xy+yz+zx-B_0, xyz-C_0)$$

and (u_1, v_1, w_1) are linearly dependent. Therefore, one of the two conditions hold:

(i) $x+y+z-A_0=0$;

(ii) $\begin{cases} xyz = \frac{w_1}{u_1}(x+y+z)+C_0-\frac{w_1}{u_1}A_0, \\ xy+yz+zx = \frac{v_1}{u_1}(x+y+z)+B_0-\frac{v_1}{u_1}A_0, \end{cases}$

If a solution (x,y,z) satisfy (i), then our congruence (22) can be written in the form

$$\Big(x+a-\frac{1}{\lambda}\Big)\Big(y+a-\frac{1}{\lambda}\Big)\Big(z+a-\frac{1}{\lambda}\Big) \equiv \lambda' \pmod p.$$

Since $\lambda \notin I^{-1} \pmod p$, we have $\lambda' \not\equiv 0 \pmod p$. Hence, by Lemma 11 the solutions counted in (i) contributes to our J at most the quantity $N^{o(1)}$.

If a solution (x,y,z) satisfy (ii), then Lemma 7 and the bound for the divisor function implies that one of the variables x,y,z is determined with at most $N^{o(1)}$ possibilities. Therefore, by Corollary 4 we get that the solutions counted on (ii) contributes to our J also at most the quantity $N^{o(1)}$.

Thus, we get $J < N^{o(1)}$ contradicting our assumption that $J > N^{\varepsilon}$. Therefore, Case 2 is impossible.

Case 3: $\lambda_1 \le 1, \lambda_2 \le 1, \lambda_3 > 1$.

Thus, $\lambda_1\lambda_2 < 1000J^{-1}$. Next,

$$\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \begin{pmatrix} a^2-2a\lambda^{-1} \\ a-\lambda^{-1} \end{pmatrix} \equiv \begin{pmatrix} -w_1 \\ -w_2 \end{pmatrix} \pmod p. \tag{24}$$

Let

$$\Delta_3 = \det\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}, \ \Delta_5 = \det\begin{pmatrix} -w_1 & v_1 \\ -w_2 & v_2 \end{pmatrix}, \ \Delta_4 = \det\begin{pmatrix} u_1 & -w_1 \\ u_2 & -w_2 \end{pmatrix}.$$

We have

$$|\Delta_3| < 2000N^3/J, \qquad |\Delta_5| < 2000N^5/J, \qquad |\Delta_4| < 2000N^4/J. \tag{25}$$

We observe that

$$\Delta_3 \not\equiv 0 \pmod p. \tag{26}$$

Indeed, assuming the contrary, from the congruence (24) we get

$$\Delta_3 \equiv \Delta_5 \equiv \Delta_4 \equiv 0 \pmod p.$$

Taking into account (25), this implies that

$$\Delta_3 = \Delta_5 = \Delta_4 = 0.$$

It then follows that the rank of the matrix

$$\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \end{pmatrix}$$

is strictly less than 2, which contradicts the linear independence of the vectors (u_i, v_i, w_i), $i = 1, 2$. Thus, we have (26). Hence,

$$a^2 - 2a\lambda^{-1} \equiv \frac{\Delta_5}{\Delta_3} \pmod p, \quad a - \lambda^{-1} \equiv \frac{\Delta_4}{\Delta_3} \pmod p.$$

Using (22), we also have

$$a^3 - 3a^2\lambda^{-1} \equiv \frac{\Delta_6}{\Delta_3} \pmod p,$$

for some integer Δ_6 with

$$|\Delta_6| < 6000N^6/J.$$

We have

$$\lambda^{-2} \equiv \frac{\Delta_4^2}{\Delta_3^2} - \frac{\Delta_5}{\Delta_3} \equiv \frac{\Delta_4^2 - \Delta_5\Delta_3}{\Delta_3^2} \pmod p. \tag{27}$$

Furthermore, substituting $\lambda^{-1} \equiv a - (\Delta_4/\Delta_3)$ in the other two equations we get

$$\Delta_3 a^2 - 2\Delta_4 a + \Delta_5 \equiv 0 \pmod p,$$
$$2\Delta_3 a^3 - 3\Delta_4 a^2 + \Delta_6 \equiv 0 \pmod p.$$

It follows that

$$\Delta_4 a^2 - 2\Delta_5 a + \Delta_6 \equiv 0 \pmod p.$$

Consider the polynomials

$$P(Z) = \Delta_4 Z^2 - 2\Delta_5 Z + \Delta_6, \quad Q(Z) = \Delta_3 Z^2 - 2\Delta_4 Z + \Delta_5.$$

Since

$$P(a) \equiv Q(a) \equiv 0 \pmod p,$$

we have

$$\mathrm{Res}(P,Q) \equiv 0 \pmod p.$$

On the other hand

$$|\mathrm{Res}(P,Q)| < 10^{18}N^{18}/J^4 < p.$$

Thus,

$$\mathrm{Res}(P,Q) = 0.$$

It then follows that the polynomials $P(Z)$ and $Q(Z)$ have a common root. If $Q(Z)$ is irreducible in $\mathbb{Q}[\mathbb{Z}]$, then $Q(Z)$ and $P(Z)$ are linearly dependent, implying that

$$\Delta_4^2 = \Delta_5\Delta_3.$$

In view of (27) this is impossible. Hence, $Q(Z)$ is irreducible in $\mathbb{Q}[\mathbb{Z}]$, and therefore its discriminant is a square of an integer. Thus,

$$\Delta_4^2 - \Delta_5\Delta_3 = m^2, \quad m \in \mathbb{Z}_+.$$

It then follows that $m < 10^4N^4/J$. Furthermore,

$$\lambda^{-2} \equiv \frac{m^2}{\Delta_3^2} \pmod p.$$

Hence,

$$\lambda^{-1} \equiv \frac{\Delta_4'}{\Delta_3} \pmod p, \quad |\Delta_4'| = m < 10^4N^4/J.$$

Consequently

$$a \equiv \frac{\Delta_4}{\Delta_3} + \lambda^{-1} \equiv \frac{\Delta_4''}{\Delta_3} \pmod p, \quad |\Delta_4''| < 10^5N^4/J.$$

$\square$

9 Proof of Theorems 1–5

9.1 Proof of Theorem 1

Let $I = [a+1, a+N]$. We first consider the case $N < p^{\frac{k+1}{2k}}$. Thus, we are aiming to prove that in this case one has the bound

$$J_{2k} < N^{2k^2/(k+1)+o(1)}.$$

Put

$$V = [N^{(k-1)/(k+1)}]; \quad Y = [N^{2/(k+1)}]; \quad I_1 = [a+1, a+2N].$$

First we define an appropriate subset $\mathcal{V} \in [0.5V,\, V]$. For a given $v \in [0.5V,\, V]$ define the function $\eta_v : I_1 \to \mathbb{Z}_+$ by

$$\eta_v(u') = \left|\left\{(u_1', v_1) \in I_1 \times [0.5V,\, V]; \quad u'v_1 \equiv u_1' v \pmod p\right\}\right|.$$

By Lemma 12,

$$\sum_{u' \in I_1} \sum_{v \in [0.5V,\, V]} \eta_v(u') < N^{1+o(1)} V.$$

Therefore, there is a subset $\mathcal{V} \in [0.5V,\, V]$ with $|\mathcal{V}| \sim V$ such that

$$\sum_{u' \in I_1} \eta_v(u') < N^{1+o(1)} \quad \text{for any} \quad v \in \mathcal{V}. \tag{28}$$

For any fixed integers $y_i \in \mathcal{Y} = [0.5Y,\, Y]$ and $v \in \mathcal{V}$ the quantity J_{2k} does not exceed the number of solutions of the congruence

$$\frac{1}{u_1' - vy_1} + \ldots + \frac{1}{u_k' - vy_k} \equiv \frac{1}{u_{k+1}' - vy_{k+1}} + \ldots + \frac{1}{u_{2k}' - vy_{2k}} \pmod p$$

in integers $u_i' \in I_1$. Thus, summing up over y_i and $v \in \mathcal{V}$ we get

$$Y^{2k} V J_{2k} \ll \frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \Big| \sum_{u' \in I_1} \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \Big|^{2k}. \tag{29}$$

For $v \in \mathcal{V}$ and B of the form $B = 2^s < N$, denote

$$S_{v,B} = \Big\{u' \in I_1; \quad 0.5B \le \eta_v(u') < B\Big\}.$$

Hence

$$I_1 = \bigcup_B S_{v,B}$$

and since $v \in \mathcal{V}$, by (28)

$$|S_{v,B}| < \frac{N^{1+o(1)}}{B}. \tag{30}$$

From (29) we clearly have

$$Y^{2k}VJ_{2k} \ll \frac{N^{o(1)}}{p}\sum_{B}\sum_{n=0}^{p-1}\sum_{v\in\mathcal{V}}\Big(\sum_{u'\in S_{v,B}}\Big|\sum_{y\in\mathcal{Y}}e_p(n(u'-vy)^{-1})\Big|\Big)^{2k}.$$

Hence, by the Hölder inequality and (30), we get, for some fixed B,

$$Y^{2k}VJ_{2k} \ll \frac{N^{o(1)}}{p}\Big(\frac{N}{B}\Big)^{2k-1}\sum_{n=0}^{p-1}\sum_{v\in\mathcal{V}}\sum_{u'\in S_{v,B}}\Big|\sum_{y\in\mathcal{Y}}e_p(n(u'-vy)^{-1})\Big|^{2k}. \qquad (31)$$

The quantity

$$\frac{1}{p}\sum_{n=0}^{p-1}\sum_{v\in\mathcal{V}}\sum_{u'\in S_{v,B}}\Big|\sum_{y\in\mathcal{Y}}e_p(n(u'-vy)^{-1})\Big|^{2k}$$

is bounded by the number of solutions of the congruence

$$\frac{1}{u'-vy_1}+\ldots+\frac{1}{u'-vy_k} \equiv \frac{1}{u'-vy_{k+1}}+\ldots+\frac{1}{u'-vy_{2k}} \pmod p$$

in variables $v\in\mathcal{V}, u'\in S_{v,B}, y\in\mathcal{Y}$. Thus, we obtain the bound

$$\frac{1}{p}\sum_{n=0}^{p-1}\sum_{v\in\mathcal{V}}\sum_{u'\in S_{v,B}}\Big|\sum_{y\in\mathcal{Y}}e_p(n(u'-vy)^{-1})\Big|^{2k} \ll Y^kV\frac{N^{1+o(1)}}{B}+Y^{2k}B.$$

Hence, from (31) we get

$$Y^{2k}VJ_{2k} \ll N^{2k-1+o(1)}B^{-2k+1}\Big(Y^kV\frac{N^{1+o(1)}}{B}+Y^{2k}B\Big)$$

Thus,

$$J_{2k} < N^{2k+o(1)}Y^{-k}+\frac{N^{2k-1+o(1)}}{V} < N^{\frac{2k^2}{k+1}+o(1)},$$

which proves the result in the case $N < p^{\frac{k+1}{2k}}$.

Let now $N > p^{\frac{k+1}{2k}}$. We split the interval $I=[a+1,a+N]$ into $K \sim Np^{-\frac{k+1}{2k}}$ subintervals of length at most $N_1 = p^{\frac{k+1}{2k}}$. Thus, for some intervals $I^{(1)},\ldots,I^{(2k)}$ of length N_1 we have the bound

$$J_{2k} < K^{2k}R_{2k} \ll \Big(\frac{N}{p^{\frac{k+1}{2k}}}\Big)^{2k}R_{2k},$$

where R_{2k} is the number of solutions of the congruence

$$\frac{1}{x_1}+\ldots+\frac{1}{x_k}\equiv\frac{1}{x_{k+1}}+\ldots+\frac{1}{x_{2k}}\pmod p,\qquad x_i\in I^{(i)},\ i=1,\ldots,2k.$$

Expressing the number of solutions of this congruence in terms of exponential sums, applying the Hölder inequality we get that

$$R_{2k}\le\prod_{i=1}^{2k}(R_{2k}(i))^{1/2k},$$

where $R_{2k}(i)$ is the number of solutions of the congruence

$$\frac{1}{x_1}+\ldots+\frac{1}{x_k}\equiv\frac{1}{x_{k+1}}+\ldots+\frac{1}{x_{2k}}\pmod p,\qquad x_1,\ldots,x_{2k}\in I^{(i)}.$$

Thus, for some fixed $i=i_0$ one has

$$R_{2k}<R_{2k}(i_0).$$

Since $|I^{(i_0)}|<N_1=p^{\frac{k+1}{2k}}$, we already know that

$$R_{2k}(i_0)<N_1^{2k^2/(k+1)+o(1)}=p^kN^{o(1)}.$$

Thus,

$$J_{2k}<\Big(\frac{N}{p^{\frac{k+1}{2k}}}\Big)^{2k}p^kN^{o(1)}=\frac{N^{2k+o(1)}}{p},$$

which concludes the proof of Theorem 1.

9.2 Proof of Theorem 2

Let $I=\{a+1,\ldots,a+N\}$. We can assume that N is large and $J>N^{2/3}\log N$, as otherwise there is nothing to prove. The conditions of Lemma 13 are satisfied, so that there exist integers Δ_4',Δ_4'' and Δ_3 with

$$|\Delta_4'|<N^{10/3},\quad|\Delta_4''|<N^{10/3},\quad|\Delta_3|<N^{7/3}$$

such that

$$a\equiv\frac{\Delta_4'}{\Delta_3}\pmod p;\quad\lambda^{-1}\equiv\frac{\Delta_4''}{\Delta_3}\pmod p.$$

Substituting this in

$$\begin{aligned}&\lambda(a+x)(a+y)(a+z)\\&\quad\equiv (a+x)(a+y)+(a+y)(a+z)+(a+z)(a+x) \pmod p\end{aligned}$$

we obtain

$$\begin{aligned}(\Delta_4'+\Delta_3 x)(\Delta_4'+\Delta_3 y)(\Delta_4'+\Delta_3 z) &\equiv \Delta_4''\Big\{(\Delta_4'+\Delta_3 x)(\Delta_4'+\Delta_3 y)\\ &+ (\Delta_4'+\Delta_3 y)(\Delta_4'+\Delta_3 z)+(\Delta_4'+\Delta_3 z)(\Delta_4'+\Delta_3 x)\Big\} \pmod p.\end{aligned}$$

The left and the right hand sides are of the order of magnitude $O(N^{10}) = o(p)$. Thus, the congruence is converted to the equality

$$\begin{aligned}(\Delta_4'+\Delta_3 x)(\Delta_4'+\Delta_3 y)(\Delta_4'+\Delta_3 z) &= \Delta_4''\Big\{(\Delta_4'+\Delta_3 x)(\Delta_4'+\Delta_3 y)\\ &+ (\Delta_4'+\Delta_3 y)(\Delta_4'+\Delta_3 z)+(\Delta_4'+\Delta_3 z)(\Delta_4'+\Delta_3 x)\Big\}\end{aligned}$$

and the claim follows from Lemma 9.

9.3 Proof of Theorem 3

Let $I = \{a+1, \ldots, a+N\}$. The statement is equivalent to the claim that for any $\varepsilon > 0$ one has the bound

$$J_6 \ll N^{3+\varepsilon},$$

where the implied constant may depend only ε.

Observe that for any $j \in \mathbb{Z}$ there are $u_j, v_j \in \mathbb{Z}$ such that

$$\frac{u_j}{v_j} \equiv j \pmod p; \quad |u_j| \le p^{1/2}, \quad 0 < |v_j| \le p^{1/2}. \tag{32}$$

This follows from the fact that among more than p numbers

$$u + jv, \quad 0 \le u, v \le [p^{1/2}]$$

there are at least two numbers congruent modulo p. We also represent a in this form, that is

$$a \equiv \frac{a_0}{b_0} \pmod p; \quad |a_0| \le p^{1/2}, \quad 0 < |b_0| \le p^{1/2}. \tag{33}$$

Let T_j be the number of solutions of the congruence

$$\frac{1}{a+x_1}+\frac{1}{a+x_2}+\frac{1}{a+x_3}\equiv j \pmod p; \quad 1\le x_1,x_2,x_3\le N.$$

We have

$$J_6=\sum_{j=0}^{p-1}T_j^2$$

and

$$\sum_{j=0}^{p-1}T_j\le N^3$$

From Corollary 4 it clearly follows that $T_j<N^{1+o(1)}$. Therefore, it follows that the contribution to J_6 from $j\in\{I^{-1}\cup 0\} \pmod p$ is

$$\sum_{\substack{0\le j\le p-1\\ j\in I^{-1}\cup 0 \pmod p}} T_j^2\le (N+1)\max_j T_J^2<N^{3+o(1)}.$$

Furthermore, the contribution to J_6 from those j for which $T_j<N^{0.1\varepsilon}$ is less than

$$N^{0.1\varepsilon}\sum_{j=0}^{p-1}T_j\le N^{3+0.1\varepsilon}.$$

Thus, if we denote by Ω the set of integers j with

$$1\le j\le p-1, \quad j\notin I^{-1} \pmod p, \quad |T_j|>N^{0.1\varepsilon},$$

then

$$J_6<N^{3+0.2\varepsilon}+\sum_{j\in\Omega}T_j^2. \tag{34}$$

Now for each j we apply Lemma 13 (where J is substituted by T_j and λ by j. Then there exist numbers $\Delta_{4j}',\Delta_{4j}'',\Delta_{3j}$ with

$$\Delta_{4j}'\ll N^4, \quad {\Delta_{4j}}''\ll N^4, \quad \Delta_{3j}\ll N^3$$

such that

$$a\equiv\frac{\Delta_{4j}'}{\Delta_{3j}} \pmod p; \qquad j^{-1}\equiv\frac{\Delta_{4j}''}{\Delta_{3j}} \pmod p.$$

Comparing this with (32) and (33), we see that

$$a \equiv \frac{a_0}{b_0} \equiv \frac{\Delta'_{4j}}{\Delta_{3j}} \pmod p; \qquad j^{-1} \equiv \frac{v_j}{u_j} \equiv \frac{\Delta''_{4j}}{\Delta_{3j}} \pmod p. \tag{35}$$

Taking into account the inequality conditions on N, a_0, b_0, u_j, v_j, we see that we have equality

$$\frac{a_0}{b_0} = \frac{\Delta'_{4j}}{\Delta_{3j}}; \qquad \frac{v_j}{u_j} = \frac{\Delta''_{4j}}{\Delta_{3j}}. \tag{36}$$

Now we represent the congruence corresponding to T_j in the form

$$\begin{aligned} x_1x_2x_3 &+ (a - j^{-1})(x_1x_2 + x_2x_3 + x_3x_1) \\ &+ (a^2 - 2aj^{-1})(x_1 + x_2 + x_3) + (a^3 - 3a^2j^{-1}) \equiv 0 \pmod p. \end{aligned}$$

Using (35), we substitute a and j^{-1}, implying

$$\begin{aligned} x_1x_2x_3 + \Big(\frac{\Delta'_{4j}}{\Delta_{3j}} - \frac{\Delta''_{4j}}{\Delta_{3j}}\Big)&(x_1x_2 + x_2x_3 + x_3x_1) \\ + \Big(\Big(\frac{\Delta'_{4j}}{\Delta_{3j}}\Big)^2 - 2\frac{\Delta'_{4j}}{\Delta_{3j}} \cdot \frac{\Delta''_{4j}}{\Delta_{3j}}\Big)&(x_1 + x_2 + x_3) \\ + \Big(\Big(\frac{\Delta'_{4j}}{\Delta_{3j}}\Big)^3 - 3\Big(\frac{\Delta'_{4j}}{\Delta_{3j}}\Big)^2 \cdot \frac{\Delta''_{4j}}{\Delta_{3j}}\Big) &\equiv 0 \pmod p. \end{aligned}$$

After multiplying by Δ_{3j}^3 the left hand side becomes an integer of the size $O(N^{12}) = o(p)$. Thus, the resulting congruence is converted to the equality, and dividing by Δ_{3j}^3 we get

$$\begin{aligned} x_1x_2x_3 + \Big(\frac{\Delta'_{4j}}{\Delta_{3j}} - \frac{\Delta''_{4j}}{\Delta_{3j}}\Big)&(x_1x_2 + x_2x_3 + x_3x_1) \\ + \Big(\Big(\frac{\Delta'_{4j}}{\Delta_{3j}}\Big)^2 - 2\frac{\Delta'_{4j}}{\Delta_{3j}} \cdot \frac{\Delta''_{4j}}{\Delta_{3j}}\Big)&(x_1 + x_2 + x_3) \\ + \Big(\Big(\frac{\Delta'_{4j}}{\Delta_{3j}}\Big)^3 - 3\Big(\frac{\Delta'_{4j}}{\Delta_{3j}}\Big)^2 \cdot \frac{\Delta''_{4j}}{\Delta_{3j}}\Big) &= 0. \end{aligned}$$

We use (36) and write this equality in the form

$$\begin{aligned} x_1x_2x_3 &+ \Big(\frac{a_0}{b_0} - \frac{v_j}{u_j}\Big)(x_1x_2 + x_2x_3 + x_3x_1) \\ &+ \Big(\frac{a_0^2}{b_0^2} - 2\frac{a_0}{b_0}\cdot\frac{v_j}{u_j}\Big)(x_1+x_2+x_3) \\ &+ \Big(\frac{a_0^3}{b_0^3} - 3\frac{a_0^2}{b_0^2}\cdot\frac{v_j}{u_j}\Big) = 0. \end{aligned}$$

Consequently we get

$$\frac{1}{(a_0/b_0)+x_1} + \frac{1}{(a_0/b_0)+x_2} + \frac{1}{(a_0/b_0)+x_3} = \frac{u_j}{v_j}. \tag{37}$$

Thus, for $j \in \Omega$ the quantity T_j is just the number of solutions of the diophantine equation (37) in positive integers $x_1, x_2, x_3 \le N$. Since u_j/v_j are pairwise distinct, we get that the quantity $\sum_{j\in\Omega} T_j^2$ is not greater than the number of solutions of the equation

$$\begin{aligned} &\frac{1}{(a_0/b_0)+x_1} + \frac{1}{(a_0/b_0)+x_2} + \frac{1}{(a_0/b_0)+x_3} \\ &\qquad = \frac{1}{(a_0/b_0)+x_4} + \frac{1}{(a_0/b_0)+x_5} + \frac{1}{(a_0/b_0)+x_6} \end{aligned}$$

in positive integers $x_1, \ldots, x_6 \le N$. Therefore, by Lemma 6 we get that

$$\sum_{j\in\Omega} T_j^2 < N^{3+o(1)}.$$

In view of (34), this completes the proof of our theorem.

9.4 Proof of Theorem 4

Let $I = \{a+1, \ldots, a+N\}$. Using standard arguments involving Hölder's inequality (combined with inductive process), it suffices to show that the contribution from the set of solutions with pairwise $x_1, \ldots, x_{2k}$ is $N^{k+o(1)}$. Thus, in what follows, we consider $x_1, \ldots, x_{2k}$ pairwise distinct.

For each solution $\vec{x} = (x_1, \ldots, x_{2k})$, we consider the polynomial $P_{\vec{x}}(Z)$ defined as

$$\prod_{i\ne 1}(Z+x_i) + \ldots + \prod_{i\ne k}(Z+x_i) - \prod_{i\ne k+1}(Z+x_i) - \ldots - \prod_{i\ne 2k}(Z+x_i).$$

Clearly, $\deg P_{\vec{x}}(Z) \le 2k-2$. Note also that $P_{\vec{x}}(-x_1) \neq 0$. In particular, $P_{\vec{x}}(Z)$ is not a zero polynomial, and since $P_{\vec{x}}(a) \equiv 0 \pmod p$, it is not a constant polynomial neither. Clearly, $P_{\vec{x}}(Z)$ has the form

$$P_{\vec{x}}(Z) = \sum_{i=0}^{2k-2} a_i Z^{2k-2-i}$$

where $|a_i| \ll N^{i+1}$. We fix one solution

$$(x_1, \ldots, x_{2k}) = (c_1, \ldots, c_{2k})$$

and consider the polynomial $P_{\vec{c}}(Z)$ that corresponds to $(c_1, \ldots, c_{2k})$. Since

$$P_{\vec{x}}(a) \equiv P_{\vec{c}}(a) \equiv 0 \pmod p,$$

we get that

$$\mathrm{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z)) \equiv 0 \pmod p.$$

On the other hand, $P_{\vec{x}}(Z)$ and $P_{\vec{c}}(Z)$ satisfy the condition of Lemma 2 with

$$\sigma = \theta = 1, \qquad m = n = 2k-1.$$

Hence,

$$\mathrm{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z)) \ll N^{4k^2-4k}.$$

Therefore, assuming $N < p^{1/(4k^2)}$, we get

$$|\mathrm{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z))| < p,$$

whence

$$\mathrm{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z)) = 0.$$

It follows that for every solution $\vec{x} = (x_1, \ldots, x_{2k})$ the polynomial $P_{\vec{x}}(Z)$ has a common root with $P_{\vec{c}}(Z)$. Since x_i are pairwise distinct, the condition $P_{\vec{x}}(\sigma) = 0$ implies that $x_i + \sigma \neq 0$. Thus, Lemma 6 implies that for every root σ of $P_{\vec{c}}(Z)$ the equation $P_{\vec{x}}(\sigma) = 0$ has at most $N^{k+o(1)}$ solutions in positive integers $x_i \le N$. The claim now follows.

9.5 Proof of Theorems 5 and 6

First we prove Theorem 5. It suffices to consider the case $kN^{k-1} < p$ as otherwise the statement is trivial. For $\lambda = 0, 1, \ldots, p-1$ denote

$$J(\lambda) = \Big\{(x_1, \ldots, x_k) \in I^k : \quad x_1^* + \ldots + x_k^* \equiv \lambda \pmod p\Big\}.$$

Let

$$\Omega = \{\lambda \in [1, p-1] : \quad |J(\lambda)| \geq 1\}.$$

Since $J(0) = 0$, we have

$$J_{2k} = \sum_{\lambda \in \Omega} |J(\lambda)|^2.$$

Consider the lattice

$$\Gamma_\lambda = \{(u, v) \in \mathbb{Z}^2 : \quad \lambda u \equiv v \pmod p\}$$

and the body

$$D = \{(u, v) \in \mathbb{R}^2 : \quad |u| \leq N^k, \ |v| \leq kN^{k-1}\}.$$

Denoting by μ_1, μ_2 the consecutive minimas of the body D with respect to the lattice Γ_λ, by Corollary 3 it follows

$$\prod_{i=1}^{2} \min\{\mu_i, 1\} \leq \frac{15}{|\Gamma_\lambda \cap D|}.$$

Observe that for $(x_1, \ldots, x_k) \in J(\lambda)$ one has

$$\lambda x_1 \ldots x_k \equiv x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1} \pmod p,$$

implying

$$(x_1 \ldots x_k, \, x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1}) \in \Gamma_\lambda \cap D.$$

Thus, for $\lambda \in \Omega$ we have $\mu_1 \leq 1$. We split the set Ω into two subsets:

$$\Omega' = \{\lambda \in \Omega : \quad \mu_2 \leq 1\}, \qquad \Omega'' = \{\lambda \in \Omega : \quad \mu_2 > 1\}.$$

We have

$$J_{2k} = \sum_{\lambda \in \Omega'} |J(\lambda)|^2 + \sum_{\lambda \in \Omega''} |J(\lambda)|^2. \tag{38}$$

Case 1: $\lambda \in \Omega'$, that is $\mu_2 \le 1$. Let $(u_i, v_i) \in \mu_i D \cap \Gamma_\lambda$, $i = 1, 2$, be linearly independent. Then

$$0 \neq \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \equiv 0 \pmod p,$$

whence

$$\left| \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \right| \ge p.$$

Also

$$\left| \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \right| \le 2k\mu_1\mu_2 N^{2k-1} \le \frac{30kN^{2k-1}}{|\Gamma \cap D|}.$$

Thus, for $\lambda \in \Omega'$, the number $|\Gamma_\lambda \cap D|$ of solutions of the congruence

$$\lambda u \equiv v \pmod p$$

in integers u, v with $|u| \le N^k$, $|v| \le kN^{k-1}$ is bounded by

$$|\Gamma_\lambda \cap D| \le \frac{30kN^{2k-1}}{p}. \tag{39}$$

Therefore, if we denote by $S(u, v)$ the set of k-tuples $(x_1, \ldots, x_k)$ of positive integers $x_1, \ldots, x_k \le N$ with

$$x_1 \ldots x_k = u, \quad x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1} = v,$$

we get

$$\sum_{\lambda \in \Omega'} |J(\lambda)|^2 = \sum_{\lambda \in \Omega'} \Big(\sum_{(u,v) \in \Gamma_\lambda \cap D} \ \sum_{(x_1, \ldots, x_k) \in S(u,v)} 1 \Big)^2.$$

Applying the Cauchy-Schwarz inequality and taking into account (39), we get

$$\sum_{\lambda \in \Omega'} |J(\lambda)|^2 = \frac{30kN^{2k-1}}{p} \sum_{\lambda \in \Omega'} \ \sum_{(u,v) \in \Gamma_\lambda \cap D} \Big(\sum_{(x_1, \ldots, x_k) \in S(u,v)} 1 \Big)^2$$

The summation on the right hand side is clearly bounded by the number of solutions of the system of equations

$$\begin{cases} x_1 \ldots x_k = y_1 \ldots y_k, \\ x_1 \ldots x_{k-1} + \ldots + x_2 \ldots x_k = y_2 \ldots y_k + \ldots + y_1 \ldots y_{k-1}, \end{cases}$$

in positive integers $x_i, y_j \le N$. Hence, by Lemma 4, it follows that

$$\sum_{\lambda\in\Omega'} |J(\lambda)|^2 < 30k(2k)^{80k^3}(\log N)^{4k^2}\frac{N^{3k-1}}{p}. \tag{40}$$

Case 2: $\lambda \in \Omega''$, that is $\mu_2 > 1$. Then the vectors from $\Gamma \cap D$ are linearly dependent and in particular there is some $\widehat{\lambda} \in \mathbb{Q}$ such that

$$\widehat{\lambda} x_1 \ldots x_k = x_2 \ldots x_k + \ldots + x_1 \ldots x_{k-1} \quad \text{for} \quad (x_1, \ldots, x_k) \in J(\lambda).$$

Thus,

$$\begin{aligned}
&\sum_{\lambda\in\Omega''} |J(\lambda)|^2 \le \sum_{\widehat{\lambda}\in\mathbb{Q}} \Big|\{(x_1,\ldots,x_k)\in I^k : \ \frac{1}{x_1}+\ldots+\frac{1}{x_k} = \widehat{\lambda}\Big|^2 \\
=&\Big|\Big\{(x_1,\ldots,x_{2k})\in[1,N]^{2k} : \quad \frac{1}{x_1}+\ldots+\frac{1}{x_k} = \frac{1}{x_{k+1}}+\ldots+\frac{1}{x_{2k}}\Big\}\Big| \\
<&(2k)^{80k^3}(\log N)^{4k^2}N^k.
\end{aligned}$$

Inserting this and (40) into (38), we obtain

$$J_{2k} < (2k)^{90k^3}(\log N)^{4k^2}\Big(\frac{N^{2k-1}}{p}+1\Big)N^k$$

which concludes the proof of Theorem 5.

The proof of Theorem 6 follows the same line with the only difference that instead of Lemma 4 one should apply the bound

$$\begin{aligned}
&\Big|\Big\{(x_1,\ldots,x_{2k})\in([1,N]\cap\mathcal{P})^{2k} : \quad \frac{1}{x_1}+\ldots+\frac{1}{x_k} = \frac{1}{x_{k+1}}+\ldots+\frac{1}{x_{2k}}\Big\}\Big| \\
&\qquad\qquad < (2k)^k\Big(\frac{N}{\log N}\Big)^k.
\end{aligned}$$

10 Proof of Theorems 7–13

10.1 Proof of Theorem 7

It suffices to deal with the case $|I_1| = [p^{1/18}]$, $|I_2| = [p^{5/12+\varepsilon}]$ and $\varepsilon < 0.1$. Let

$$W_2 = \sum_{x_1\in I_1}\sum_{x_2\in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*).$$

We take $k = [1/\varepsilon]$ and apply the Hölder inequality;

$$
\begin{aligned}
|W_2|^k \leq & |I_1|^{k-1} \sum_{x_1 \in I_1} \Big| \sum_{x_2 \in I_2} \alpha_2(x_2) e_p(a x_1^* x_2^*) \Big|^k \\
= & |I_1|^{k-1} \sum_{x_1 \in I_1} \Big| \sum_{y_1, \ldots, y_k \in I_2} \alpha_2(y_1) \ldots \alpha_2(y_k) e_p(a x_1^* (y_1^* + \ldots + y_k^*)) \Big| \\
= & |I_1|^{k-1} \sum_{x_1 \in I_1} \theta(x_1) \Big(\sum_{y_1, \ldots, y_k \in I_2} \alpha_2(y_1) \ldots \alpha_2(y_k) e_p(a x_1^* (y_1^* + \ldots + y_k^*)) \Big) \\
\leq & |I_1|^{k-1} \sum_{y_1, \ldots, y_k \in I_2} \Big| \sum_{x_1 \in I_1} \theta(x_1) e_p(a x_1^* (y_1^* + \ldots + y_k^*)) \Big|,
\end{aligned}
$$

where $\theta(x)$ some complex numbers with $|\theta(x)| \leq 1$. We again apply the Hölder inequality and obtain

$$
\begin{aligned}
|W_2|^{3k} \leq & |I_1|^{3k-3} |I_2|^{2k} \sum_{y_1, \ldots, y_k \in I_2} \Big| \sum_{x_1 \in I_1} \theta(x_1) e_p(a x_1^* (y_1^* + \ldots + y_k^*)) \Big|^3 \\
= & |I_1|^{3k-3} |I_2|^{2k} \sum_{\lambda=0}^{p-1} T(\lambda) \Big| \sum_{x_1 \in I_1} \theta(x_1) e_p(a x_1^* \lambda) \Big|^3,
\end{aligned}
$$

where $T(\lambda)$ is the number of solutions of the congruence

$$
y_1^* + \ldots + y_k^* \equiv \lambda \pmod p, \quad y_i \in I_2.
$$

We apply now the Cauchy-Schwarz inequality and get

$$
|W_2|^{6k} \leq |I_1|^{6k-6} |I_2|^{4k} \Big(\sum_{\lambda=0}^{p-1} T(\lambda)^2 \Big) \sum_{\lambda=0}^{p-1} \Big| \sum_{x_1 \in I_1} \theta(x_1) e_p(a x_1^* \lambda) \Big|^6.
$$

By Theorem 1, we have

$$
\sum_{\lambda=0}^{p-1} T(\lambda)^2 < |I_2|^{2k-2+1/(k+1)+o(1)} < |I_2|^{2k-2+\varepsilon}.
$$

Furthermore,

$$
\sum_{\lambda=0}^{p-1} \Big| \sum_{x_1 \in I_1} \theta(x_1) e_p(a x_1^* \lambda) \Big|^6 \leq p J_6,
$$

where J_6 is the number of solutions of the congruence

$$y_1^* + y_2^* + y_3^* \equiv y_4^* + y_5^* + y_6^* \pmod p, \quad y_i \in I_1.$$

By Theorem 3, we have $J_6 = |I_1|^{3+o(1)}$. Thus,

$$|W_2|^{6k} \le p|I_1|^{6k-3+o(1)}|I_2|^{6k-2+\varepsilon}.$$

Since $p \ll |I_1|^3|I_2|^2p^{-2\varepsilon}$, the result follows.

10.2 Proof of Theorems 8, 9, 10

Let

$$S = \sum_{x_1\in I_1}\sum_{x_2\in I_2} \alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^*x_2^*).$$

Then by Hölder's inequality

$$|S|^{k_2} \le N_1^{k_2-1} \sum_{x_1\in I_1}\Big|\sum_{x_2\in I_2} \alpha_2(x_2)e_p(ax_1^*x_2^*)\Big|^{k_2}.$$

Thus, for some $\sigma(x_1) \in \mathbb{C}$, $|\sigma(x_1)| = 1$,

$$|S|^{k_2} \le N_1^{k_2-1} \sum_{y_1,\ldots,y_{k_2}\in I_2}\Big|\sum_{x_1\in I_1} \sigma(x_1)e_p(ax_1^*(y_1^*+\ldots+y_{k_2}^*)\Big|.$$

Again by Hölder's inequality,

$$|S|^{k_1k_2} \le N_1^{k_1k_2-k_1}N_2^{k_1k_2-k_2}\sum_{\lambda=0}^{p-1} J_{k_2}(\lambda;N_2)\Big|\sum_{x_1\in I_1}\sigma(x_1)e_p(ax_1^*\lambda\Big|^{k_1},$$

where $J_k(\lambda;N)$ is the number of solutions of the congruence

$$x_1^* + \ldots + x_k^* \equiv \lambda \pmod p, \qquad x_i \in [1,N].$$

Then applying the Cauchy-Schwarz inequality and using

$$\sum_{\lambda=0}^{p-1} J_{k_2}(\lambda;N_2)^2 = J_{2k_2}(N_2), \qquad \sum_{\lambda=0}^{p-1}\Big|\sum_{x_1\in I_1}\sigma(x_1)e_p(ax_1^*\lambda\Big|^{2k_1} \le pJ_{2k_1}(N_1).$$

we get

$$|S|^{2k_1k_2} \le pN_1^{2k_1k_2-2k_1}N_2^{2k_1k_2-2k_2}J_{2k_1}(N_1)J_{2k_2}(N_2). \tag{41}$$

Applying Theorem 5, we obtain

$$\begin{aligned}|S|^{2k_1k_2} \le &(2k_1)^{90k_1^3}(2k_2)^{90k_2^3}(\log N_1)^{4k_1^2}(\log N_2)^{4k_2^2}\times \\ &\times N_1^{2k_1k_2}N_2^{2k_1k_2}\Big(\frac{N_1^{k_1-1}}{p^{1/2}}+\frac{p^{1/2}}{N^{k_1}}\Big)\Big(\frac{N_2^{k_2-1}}{p^{1/2}}+\frac{p^{1/2}}{N^{k_2}}\Big).\end{aligned}$$

Thus,

$$\begin{aligned}|S| < &(2k_1)^{45k_1^2/k_2}(2k_2)^{45k_2^2/k_1}(\log p)^{2(\frac{k_1}{k_2}+\frac{k_2}{k_1})}\times \\ &\times\Big(\frac{N_1^{k_1-1}}{p^{1/2}}+\frac{p^{1/2}}{N^{k_1}}\Big)^{1/(2k_1k_2)}\Big(\frac{N_2^{k_2-1}}{p^{1/2}}+\frac{p^{1/2}}{N^{k_2}}\Big)^{1/(2k_1k_2)}N_1N_2,\end{aligned}$$

which finishes the proof of Theorem 8.

To prove Theorem 9, we note that if $1 \le N < p$, then as a consequence of Corollary 4, the number of solutions of the congruence

$$\frac{1}{x_1}+\frac{1}{x_2} \equiv \frac{1}{x_3}+\frac{1}{x_4} \pmod p, \quad L+1 \le x_1,x_2,x_3,x_4 \le L+N$$

is bounded by $N^{2+o(1)}(N^{3/2}p^{-1/2}+1)$. Following the proof of Theorem 8 with $k_1 = k_2 = 2$ and applying this bound with $[L+1, L+N] = I_i$, we derive Theorem 9.

To prove Theorem 10 we use (41), where in this case $J_{2k_i}(N_i)$ is the number of solutions of the congruence

$$x_1^{-1}+\ldots+x_k^{-1} = x_{k+1}^{-1}+\ldots+x_{2k}^{-1}, \qquad (x_1,\ldots,x_{2k}) \in I_i^{2k}.$$

Since

$$N_1 < p^{\frac{k_1+1}{2k_1}}, \qquad N_2 < p^{\frac{k_2+1}{2k_2}},$$

by Theorem 1 we have

$$J_{2k_1}(N_1) < N_1^{\frac{2k_1^2}{k_1+1}}, \qquad J_{2k_2}(N_2) < N_2^{\frac{2k_2^2}{k_2+1}}.$$

Incorporating this in (41), the result follows.

10.3 Proof of Theorem 11

Denote
$$W_n = \Big|\sum_{x_1\in I_1}\dots\sum_{x_n\in I_n}\alpha_1(x_1)\dots\alpha_n(x_n)e_p(ax_1^*\dots x_n^*)\Big|.$$
Applying n times the Hölder inequality and using that for $|\alpha(v)|\le 1$ one has
$$\sum_u\Big|\sum_v\alpha(v)e_p(auv)\Big|^6 \le \sum_{v_1,\dots,v_6}\Big|\sum_u e_p(a(v_1+v_2+v_3-v_4-v_5-v_6)u)\Big|,$$
it follows that
$$W_n^{6^n}\le N^{n6^n-6n}\times$$
$$\times\sum_{x_{11},\dots,x_{16}\in I_1}\dots\sum_{x_{n1},\dots x_{n6}\in I_n} e_p(a(x_{11}^*+\dots-x_{16}^*)\dots(x_{n1}^*+\dots-x_{n6}^*)).$$
We can fix x_{j4},x_{j5},x_{j6} such that for some integers c_j
$$W_n^{6^n}\le N^{n6^n-3n}\Big|\sum_{x_{11},x_{12},x_{13}\in I_1}\dots\sum_{x_{n1},x_{n2},x_{n3}\in I_n}\{...\}\Big|$$
where in the brackets $\{...\}$ we have the expression
$$e_p(a(x_{11}^*+x_{12}^*+x_{13}^*-c_1)\dots(x_{n1}^*+x_{n2}^*+x_{n3}^*-c_n)).$$
Let $T_j(\lambda)$, $j=1,\dots,n$, be the number of solutions of the congruence
$$x_1^*+x_2^*+x_3^*-c_j\equiv\lambda \pmod p,\quad x_1,x_2,x_3\in I_j.$$
Then we get
$$W_n^{6^n}\le N^{n6^n-3n}\Big|\sum_{\lambda_1=0}^{p-1}\dots\sum_{\lambda_n=0}^{p-1}T_1(\lambda_1)\dots T_n(\lambda_n)e_p(a\lambda_1\dots\lambda_n)\Big|. \tag{42}$$
Now we observe that
$$\sum_{\lambda=0}^{p-1}\frac{T_j(\lambda)}{N^3}\le 1$$
and also by Theorem 3 we have
$$\sum_\lambda\Big(\frac{T_j(\lambda)}{N^3}\Big)^2<N^{-3+o(1)}.$$

Furthermore,

$$\prod_{j=1}^{n}\Big(\sum_{\lambda}\Big(\frac{T_j(\lambda)}{N^3}\Big)^2\Big)^{1/2} < N^{-3n/2+o(1)} < p^{-1/2-\delta}$$

for some $\delta = \delta(\varepsilon, n) > 0$. Thus, we can apply Lemma 1 with

$$\gamma_j(x) = \frac{T_j(x)}{N^3}.$$

This implies that

$$\Big|\sum_{\lambda_n=0}^{p-1} T_1(\lambda_1)\ldots T_n(\lambda_n)e_p(a\lambda_1\ldots\lambda_n)\Big| < N^{3n}p^{-\delta'}.$$

Inserting this into (42), we conclude the proof.

10.4 Proof of Theorem 12

Let $c \le 1/4$ be the constant that satisfies Theorem 4 and take $C = 9c^{-2}$. In particular, we can assume that $n > 3c^{-1}$. Clearly, we can also assume that $N = [p^{9/(cn^2)}]$. For $k = [cn/3]$ we have

$$p^{c/k^2} \ge p^{9/(cn^2)} > N.$$

Thus, for every j the number of solutions of the congruence

$$y_1^* + \ldots + y_k^* \equiv y_{k+1}^* + \ldots + y_{2k}^* \pmod p, \quad y_1, \ldots, y_{2k} \in I_j,$$

is bounded by $N^{k+o(1)}$. Letting

$$W_n = \Big|\sum_{x_1\in I_1}\cdots\sum_{x_n\in I_n}\alpha_1(x_1)\ldots\alpha_n(x_n)e_p(ax_1^*\ldots x_n^*)\Big|,$$

we have

$$W_n^{(2k)^n} \le N^{n(2k)^n-2kn}\sum_{x_{11},\ldots,x_{(2k)1}\in I_1}\cdots\sum_{x_{1n},\ldots,x_{(2k)n}\in I_n} e_p(a\{...\})$$

where $\{...\}$ denotes

$$\prod_{j=1}^{n}(x_{1j}^* + \ldots + x_{kj}^* - x_{(k+1)j}^* - \ldots - x_{(2k)j}^*).$$

We can fix $x_{(k+i)j}$ for all $i = 1, \ldots, k$ and $j = 1, \ldots, n$ such that for some integers $c_1, \ldots, c_n$ we have

$$W_n^{(2k)^n} \le N^{n(2k)^n - kn} \Big| \sum_{x_{11}, \ldots, x_{k1} \in I_1} \cdots \sum_{x_{1n}, \ldots, x_{kn} \in I_n} e_p(a\{...\}) \Big|$$

where $\{...\}$ denotes

$$(x_{11}^* + \ldots + x_{k1}^* - c_1) \ldots (x_{1n}^* + \ldots + x_{kn}^* - c_n).$$

Thus,

$$W_n^{(2k)^n} \le N^{n(2k)^n - kn} \Big| \sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \ldots T_n(\lambda_n) e_p(a\lambda_1 \ldots \lambda_n) \Big|, \qquad (43)$$

where $T_j(\lambda_j)$ is the number of solutions of the congruence

$$y_1^* + \ldots + y_k^* - c_j \equiv \lambda_j \pmod p, \quad (y_1, \ldots, y_k) \in I_j^k.$$

We have

$$\sum_{\lambda_j=0}^{p-1} \frac{T_j(\lambda_j)}{N^k} \le 1.$$

Furthermore, by Theorem 4

$$\sum_{\lambda_j=0}^{p-1} \Big(\frac{T_j(\lambda_j)}{N^k}\Big)^2 < \frac{N^{k+o(1)}}{N^{2k}} < N^{-k+o(1)} < p^{-\delta}$$

and

$$\prod_{j=1}^{n} \Big(\sum_{\lambda_j=0}^{p-1} \Big(\frac{T_j(\lambda_j)}{N^k}\Big)^2 \Big)^{1/2} < N^{-kn/2} p^{o(1)} < p^{-1/2-\delta}$$

for some $\delta = \delta(\varepsilon, n) > 0$. Here we used that

$$N = [p^{9/(cn^2)}]; \qquad N^{kn/2} > N^{cn^2/12} \gg p^{3/4}.$$

Thus, we can apply Lemma 1, leading to

$$\sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \ldots T_n(\lambda_n) e_p(a\lambda_1 \ldots \lambda_n) < N^{2kn} p^{-\delta'}$$

for some $\delta' = \delta'(\varepsilon, n) > 0$. Joining this with (43), we conclude the proof of Theorem 12.

10.5 Proof of Theorem 13

Put $N_j = |I_j|$. Removing, if necessary, intervals I_j with $N_j \le p^{\varepsilon/(2n)}$ we can easily reduce the problem to the case when $N_j > p^{\varepsilon/(2n)}$ for all j and $N_1 \dots N_n \ge p^{1/2+\varepsilon}$. Also note that if $N_j \ge p^{1/2+\varepsilon/(10n)}$, then the claim follows from Weil's bound for incomplete Kloosterman sums. Thus, we can also assume that $N_j < p^{1/2+\varepsilon/(10n)}$ for all j. Then those intervals I_j for which $N_j > p^{1/2}$ we refine to subintervals of sizes $\approx p^{1/2}$ and thus can assume that $p^{\varepsilon/(2n)} < N_j < p^{1/2}$ for all j. Again we can refine the intervals in an obvious way and eventually reduce the problem to the case when

$$p^{1/2+\varepsilon} < N_1 \dots N_n < 2p^{1/2+\varepsilon}$$

and

$$p^{\varepsilon/(2n)} < N_j < p^{1/2}, \quad j = 1, 2, \dots, n.$$

Let

$$W_n = \Big| \sum_{x_1 \in I_1} \dots \sum_{x_n \in I_n} \alpha_1(x_1) \dots \alpha_n(x_n) e_p(a x_1^* \dots x_n^*) \Big|.$$

Taking $k = [2/\varepsilon]$ and consequently applying Hölder's inequality n times, we get

$$\begin{aligned} W_n^{(2k)^n} \le & (N_1 \dots N_n)^{(2k)^n - 2k} \times \\ & \sum_{\lambda_1=0}^{p-1} \dots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \dots T_n(\lambda_n) e_p(a\lambda_1 \dots \lambda_n), \end{aligned} \tag{44}$$

where $T_j(\lambda_j)$ is the number of solutions of the congruence

$$(y_1^* + \dots + y_k^*) - (y_{k+1}^* + \dots + y_{2k}^*) \equiv \lambda_j \pmod p, \quad (y_1, \dots, y_{2k}) \in I_j^{2k}.$$

Now we observe that

$$\sum_{\lambda_j=0}^{p-1} \frac{T_j(\lambda_j)}{N_j^{2k}} \le 1.$$

Furthermore, by Theorem 1

$$\sum_{\lambda_j=0}^{p-1} \Big(\frac{T_j(\lambda_j)}{N_j^{2k}} \Big)^2 < \frac{N_j^{4k-2+1/(2k+1)+o(1)}}{N_j^{4k}} < N_j^{-2+1/(2k+1)+o(1)} < p^{-\delta}$$

and

$$\prod_{j=1}^{n}\Big(\sum_{\lambda_j=0}^{p-1}\Big(\frac{T_j(\lambda_j)}{N_j^{2k}}\Big)^2\Big)^{1/2} < (N_1\dots N_n)^{-1}p^{0.5\varepsilon} < p^{-1/2-\delta}$$

for some $\delta = \delta(\varepsilon, n) > 0$. Thus, we can apply Lemma 1, leading to

$$\sum_{\lambda_1=0}^{p-1}\dots\sum_{\lambda_n=0}^{p-1} T_1(\lambda_1)\dots T_n(\lambda_n)e_p(a\lambda_1\dots\lambda_n) < (N_1\dots N_n)^{2k}p^{-\delta'}$$

for some $\delta' = \delta'(\varepsilon, n) > 0$. Joining this with (44), we conclude the proof of Theorem 13.

11 Proof of Theorem 14

We need the following consequence of [7, Theorem 7]. Let μ, ν be positive probability measures on $\mathbb{R}$ supported on $[-1, 1]$, α, β complex functions on $\mathbb{R}$; $|\alpha|, |\beta| \le 1$. Let $\xi \in \mathbb{R}$, $|\xi| > 1$. Then

$$\Big|\int\int \alpha(x)\beta(y)e^{ixy\xi}\mu(dx)\nu(dy)\Big| \ll |\xi|^{-1/2}\,\|\mu * \varphi_\delta\|_2\,\|\nu * \varphi_\delta\|_2, \qquad (45)$$

where $\delta = (100|\xi|)^{-1}$ and

$$\varphi_\delta(t) = \begin{cases} \delta^{-1} & \text{if} \quad t \in [-\frac{\delta}{2}, \frac{\delta}{2}], \\ 0 & \text{otherwise.} \end{cases}$$

Note that (45) is very simple, the paper [7] contains also multi-linear versions derived from discretized ring theorem, but we do not need them here.

Let us give a direct proof of (45). For the brevity write $\varphi = \varphi_\delta$. Since

$$\widehat{\varphi}(\lambda) = \frac{2}{\delta\lambda}\sin\frac{\delta\lambda}{2}$$

we have, for $|\lambda| < (10\delta)^{-1} = 10\xi$ and $|y| \le 1$,

$$\frac{1}{2} < \widehat{\varphi}(\lambda) \le 1, \qquad \Big|\frac{\beta(y)}{\widehat{\varphi}(\xi y)}\Big| \le 2.$$

Write for $x, y \in [-1, 1]$

$$e^{i\xi xy} = \frac{1}{\widehat{\varphi}(\xi y)}\int \varphi(s - x)e^{i\xi sy}ds.$$

Hence,

$$\begin{aligned} &\Big|\int\int \alpha(x)\beta(y)e^{ixy\xi}\mu(dx)\nu(dy)\Big| \leq \\ &\int\int\Big|\int \frac{\beta(y)}{\widehat{\varphi}(\xi y)}e^{i\xi sy}\nu(dy)\Big|\varphi(s-x)\mu(dx)ds = \\ &\quad\int \widehat{\nu_1}(\xi s)(\mu * \varphi)(s)ds, \end{aligned} \tag{46}$$

where

$$\frac{d\nu_1}{d\nu} = \frac{\beta(y)}{\widehat{\varphi}(\xi y)}, \quad \text{hence} \quad |\nu_1| \leq 2\nu.$$

Since $\operatorname{supp}(\mu * \varphi) \subset [-2, 2]$, it follows from (46) that

$$\Big|\int\int \alpha(x)\beta(y)e^{ixy\xi}\mu(dx)\nu(dy)\Big| \leq \|\mu * \phi\|_2 \ \|\widehat{\nu_1}(\xi\cdot)\|_{L^2[-2,2]}.$$

Next, for $|s| \leq 2$

$$|\widehat{\nu_1}(\xi s)| \leq 2|\widehat{\nu_1}(\xi s)\widehat{\varphi}(\xi s)| = 2|(\nu_1 * \varphi)\widehat{\ }\,(\xi s)|.$$

Therefore

$$\begin{aligned} \|\widehat{\nu_1}(\xi\cdot)\|_{L^2[-2,2]} &\leq 2|\xi|^{-1/2}\|(\nu_1 * \varphi)\widehat{\ }\,\|_2 \\ &= 2|\xi|^{-1/2}(2\pi)^{1/2}\|\nu_1 * \varphi\|_2 \\ &\leq 4(2\pi)^{1/2}|\xi|^{-1/2}\|\nu * \varphi\|_2, \end{aligned}$$

and inequality (45) follows.

Let $e(z) = e^{iz}$. Denoting

$$S = \sum_{\substack{n_1 \sim N_1 \\ n_2 \sim N_2}} e\Big(\frac{1}{n_1}\frac{1}{n_2}\,\xi\Big),$$

we estimate

$$\begin{aligned} |S|^{k_1k_2} \leq N_1^{k_1k_2-k_1}N_2^{k_1k_2-k_2} \times \\ \times \sum_{\substack{n_{11},\ldots,n_{1k_1} \sim N_1 \\ n_{21},\ldots,n_{2k_2} \sim N_2}} \alpha_{\overline{n_1}}\,\beta_{\overline{n_2}}\,e\Big(\xi\Big(\frac{1}{n_{11}} + \ldots + \frac{1}{n_{1k_1}}\Big)\Big(\frac{1}{n_{21}} + \ldots + \frac{1}{n_{2k_2}}\Big)\Big), \end{aligned}$$

where $\overline{n_i} = (n_{i1}, \dots, n_{ik_i})$ and

$$\alpha_{\overline{n_1}} = \alpha_{(\frac{1}{n_{11}}+\dots+\frac{1}{n_{1k_1}})}, \quad \beta_{\overline{n_2}} = \beta_{(\frac{1}{n_{21}}+\dots+\frac{1}{n_{2k_2}})}$$

and $|\alpha_{\overline{n_1}}| = |\beta_{\overline{n_2}}| = 1$. Thus, for some complex coefficients $\alpha(x)$ and $\beta(y)$ with $|\alpha(x)| = |\beta(y)| = 1$ we have

$$|S|^{k_1k_2} \leq (N_1N_2)^{k_1k_2} \Big| \int \int \alpha(x)\beta(y) e\Big(\frac{\xi}{N_1N_2} xy\Big) \mu(dx)\nu(dy) \Big|,$$

where μ is obtained as normalized image measure on $\mathbb{R}$ under the map

$$\{n_i \sim N_1\}^{k_1} \to \mathbb{R}: \quad (n_{11}, \dots, n_{1k_1}) \to N_1 \Big(\frac{1}{n_{11}} + \dots + \frac{1}{n_{1k_1}}\Big)$$

and similarly for ν.

Set $\delta = \frac{N_1N_2}{100|\xi|}$. It follows from (45) that

$$|S|^{k_1k_2} \leq (N_1N_2)^{k_1k_2} \delta^{1/2} \|\mu * \varphi_\delta\|_2 \, \|\nu * \varphi_\delta\|_2. \tag{47}$$

Next we estimate $\|\mu * \varphi_\delta\|_2$. Note that if I_j is a partition of $\mathbb{R}$ in δ-intervals, then

$$\sum_j \Big|(n_1, \dots, n_k);\ n_i \sim N \quad \text{and} \quad \frac{N}{n_1} + \dots + \frac{N}{n_k} \in I_j \Big| \leq$$
$$\Big|(n_1, \dots, n_{2k});\ n_i \sim N \quad \text{and} \quad \Big| \frac{1}{n_1} + \dots + \frac{1}{n_k} - \frac{1}{n_{k+1}} - \dots - \frac{1}{n_{2k}} \Big| < \frac{\delta}{N} \Big|.$$

Thus, it follows that

$$\|\mu * \varphi_\delta\|_2^2 \sim N_1^{-2k_1} \delta^{-1} T(N_1), \tag{48}$$

where

$$T(N) = \Big|(n_1, \dots, n_{2k});\ n_i \sim N \text{ and } \Big| \frac{1}{n_1} + \dots + \frac{1}{n_k} - \frac{1}{n_{k+1}} - \dots - \frac{1}{n_{2k}} \Big| < \frac{\delta}{N} \Big|.$$

Let us prove that

$$T(N) < c(k)(\log N)^{4k^2} N^k (1 + \delta N^{2k-1}).$$

For $\lambda \in \mathbb{Q}$, denote $J(\lambda)$ the number of solutions of representations of λ as

$$\lambda = \frac{1}{n_1} + \ldots + \frac{1}{n_k}, \quad n_i \sim N. \tag{49}$$

By Lemma 4,

$$\sum_\lambda J(\lambda)^2 \leq c(k) N^k (\log N)^{4k^2}.$$

Also note that different λ's are at least $\sim N^{-2k}$ separated. Hence an interval $I \subset \mathbb{R}$ of size δ/N contains at most $1 + N^{2k-1}\delta$ elements of the form (49). Therefore,

$$\begin{aligned} T(N) \leq & \sum_{n_1,\ldots,n_k \sim N} J\Big(\frac{1}{n_1} + \ldots + \frac{1}{n_k}\Big)(1 + N^{2k-1}\delta) \\ \leq & (1 + N^{2k-1}\delta) \sum_\lambda J(\lambda)^2 < c(k) N^k (\log N)^{4k^2} (1 + N^{2k-1}\delta), \end{aligned}$$

which establishes the required bound for $T(N)$.

Thus, from (48) we get

$$\|\mu * \varphi_\delta\|_2 \leq c(k_1)(\log N_1)^{2k_1} \delta^{-1/2} N_1^{-k_1/2} (1 + \delta N_1^{2k_1-1})^{1/2}.$$

Similarly,

$$\|\nu * \varphi_\delta\|_2 \leq c(k_2)(\log N_2)^{2k_2} \delta^{-1/2} N_2^{-k_2/2} (1 + \delta N_2^{2k_2-1})^{1/2}.$$

Inserting these bounds into (47), we get

$$\begin{aligned} |S|^{k_1 k_2} \leq & c(k_1) c(k_2) (\log N_1)^{2k_1} (\log N_2)^{2k_2} (N_1 N_2)^{k_1 k_2} \times \\ & \times \Big(\delta^{-1/2} N_1^{-k_1} + \delta^{1/2} N_1^{k_1-1}\Big)^{1/2} \Big(\delta^{-1/2} N_2^{-k_2} + \delta^{1/2} N_2^{k_2-1}\Big)^{1/2}. \end{aligned}$$

Recalling that $\delta = \frac{N_1 N_2}{100|\xi|}$ we conclude the proof.

12 Some applications

In this section we apply Theorem 14 to prove Theorem 15 on $\pi(x) - \pi(x-y)$, and apply trilinear exponential sum bounds to prove Theorem 16 on a linear Kloosterman sums and Theorem 17 on Brun-Titchmarsh theorem.

12.1 Proof of Theorem 15

In view of Huxley's result [21] we can assume that $y < x^{7/12+}$. The function

$$\frac{2(1-\theta)}{12(\theta^{-1}+1)(\theta^{-1}+0.5)+1-\theta}$$

increases in $\theta \in [0, 7/12]$, so we can assume that $y = x^{\theta}$. Going over the argument of [18, p.269], (13.56) gives a bound on $R(M,N)$ of the form

$$\frac{Hy}{MN}\Big|\sum_{\substack{m\sim M\\ n\sim N}} \alpha_m \beta_n e\Big(\frac{hu}{mn}\Big)\Big|$$

with $u \sim x$ and $1 \leq h \leq H = MNy^{-1}x^{\varepsilon}$. Here M, N may be chosen arbitrarily with

$$MN = D > y$$

(see [18, Theorem 12.21]) and we need to ensure that

$$R(M,N) < yx^{-\varepsilon}.$$

We may then state an upper bound

$$\pi(x) - \pi(x-y) < \frac{2y}{\log D}.$$

Thus,

$$\frac{Hy}{MN}\Big|\sum_{\substack{m\sim M\\ n\sim N}} \alpha_m \beta_n e\Big(\frac{hu}{mn}\Big)\Big| \leq x^{\varepsilon}\Big|\sum_{\substack{m\sim M\\ n\sim N}} \alpha_m \beta_n e\Big(\frac{\xi}{mn}\Big)\Big|, \tag{50}$$

where

$$D < x \leq \xi < \frac{D}{y}x^{1+\varepsilon}.$$

Take k satisfying

$$k - \frac{1}{2} < \frac{1}{\theta} < k + \frac{1}{2}$$

and define M by

$$\frac{x}{D} = M^{2k-1}.$$

Let

$$N = \frac{D}{M}$$

and choose l such that

$$N^{2(l-1)} \le \frac{\xi}{D} < N^{2l}.$$

Hence,

$$\log N = \log D - \frac{\log \frac{x}{D}}{2k-1} \ge \log y - \frac{\log \frac{x}{y}}{2k-1} = \Big(\theta - \frac{1-\theta}{2k-1}\Big)\log x > \frac{\theta}{2}\log x$$

and $l \le \theta^{-1}+1$. Bounding (50) by Theorem 14 gives

$$\begin{aligned}
&x^\varepsilon D\Big(\frac{\xi}{D}M^{-2k} + \frac{D}{\xi}M^{2(k-1)}\Big)^{1/(4kl)} \le \\
&x^\varepsilon D\Big(\frac{Dx^\varepsilon}{y}M^{-1} + M^{-1}\Big)^{1/(4kl)} < \\
&x^{2\varepsilon}\Big(\frac{D}{y}\Big)^{5/4}\Big(\frac{x}{D}\Big)^{-1/(4k(2k-1)l)} y < \\
&x^{2\varepsilon}\Big(\frac{D}{y}\Big)^{3/2} x^{-\frac{(1-\theta)\theta}{8(\theta^{-1}+1)(\theta^{-1}+0.5)}} y.
\end{aligned}$$

Hence we may take

$$D = y^{1+\frac{1-\theta}{12(\theta^{-1}+1)(\theta^{-1}+0.5)}-\varepsilon'}$$

implying Theorem 15.

12.2 Proof of Theorem 16

Denote $\varepsilon = \log N/\log p$. As a consequence of the Weil bound on incomplete Kloosterman sums, we can assume that $\varepsilon < 4/7$. Let

$$\mathcal{G} = \{x < N : \quad p_1 \ge N^\alpha,\, p_3 \ge N^\beta,\, p_1p_2p_3 < N^{1-\beta}\},$$

where $p_1 \ge p_2 \ge p_3$ are the largest prime factors of x and

$$0.1 > \alpha > \beta > \frac{1}{\log N}$$

are parameters to specify. Letting $0.1 > \beta_1 > \beta$ be another parameter, we observe that

$$\sum_{\substack{x<N\\ p_1p_2>N^{1-\beta_1}}} 1 \le \sum_{y<N^{\beta_1}}\sum_{p_1p_2\le N/y} 1 \le \sum_{y<N^{\beta_1}}\sum_{p_2\le N} \frac{3N}{p_2 y\log N} \le 4\beta_1(\log\log N)N.$$

Similarly,

$$\sum_{\substack{x<N\\ p_1p_2p_3\ge N^{1-\beta}}} 1 < \sum_{y\le N^\beta}\sum_{p_2p_3<N} \frac{4N}{yp_2p_3\log N} < 5\beta(\log\log N)^2 N.$$

We also note that the number of positive integers not exceeding N and consisting on products of at most two prime numbers is less than

$$\frac{2N\log\log N}{\log N} < 2\beta N\log\log N.$$

Hence, we have

$$\begin{aligned} N-|\mathcal{G}| \le & \frac{2N\log\log N}{\log N} + \\ & + \sum_{\substack{x<N\\ p_1<N^\alpha}} 1 + \sum_{\substack{x<N\\ p_1p_2>N^{1-\beta_1}}} 1 + \sum_{\substack{x<N\\ p_1p_2\le N^{1-\beta_1}\\ p_3<N^\beta}} 1 + \sum_{\substack{x<N\\ p_1p_2p_3\ge N^{1-\beta}}} 1 \\ & \le \frac{2N\log\log N}{\log N} + \Psi(N,N^\alpha) + 4\beta_1 N\log\log N \\ & + \sum_{p_1p_2<N^{1-\beta_1}} \Psi\Big(\frac{N}{p_1p_2}, N^\beta\Big) + 5\beta N(\log\log N)^2. \end{aligned}$$

Here $\Psi(x,y)$, as usual, denotes the number of positive integers $\le x$ having no prime divisors $> y$. By the classical result of de Bruin [10] if $y > (\log x)^{1+\delta}$, where $\delta > 0$ is a fixed constant, then

$$\Psi(x,y) \le xu^{-u(1+o(1))} \quad \text{as} \quad u = \frac{\log x}{\log y} \to \infty.$$

Thus, taking

$$\alpha = \frac{1}{\log\log p}, \qquad \beta_1 = \beta\log\log p, \qquad \frac{2\log\log N}{\log N} < \beta < \frac{1}{(\log\log p)^3},$$

we have

$$\begin{aligned} N-|\mathcal{G}| < \alpha^{\frac{1}{2\alpha}} N + \sum_{p_1p_2<N^{1-\beta_1}} \frac{N}{p_1p_2}\Big(\frac{\beta}{\beta_1}\Big)^{\frac{\beta_1}{2\beta}} + 11\beta N(\log\log p)^2 \\ < \Big(\alpha^{\frac{1}{2\alpha}} + (\log\log N)^2\Big(\frac{\beta}{\beta_1}\Big)^{\frac{\beta_1}{2\beta}} + 11\beta(\log\log p)^2\Big) N \\ < 12\beta(\log\log p)^2 N. \end{aligned}$$

Therefore

$$\Big|\sum_{x<N} e_p(ax^*)\Big| \le 12\beta(\log\log p)^2 N + \Big|\sum_{x\in\mathcal{G}} e_p(ax^*)\Big|.$$

We can further assume that

$$\varepsilon\beta > \frac{1}{\sqrt{\log p}}.$$

The sum $\sum_{x\in\mathcal{G}} e_p(ax^*)$ may be bounded by

$$\sum_{p_1}\sum_{p_2}\sum_{p_3}\Big|\sum_{y} e_p(ap_1^*p_2^*p_3^*y^*)\Big|, \tag{51}$$

where the summations are taken over primes p_1, p_2, p_3 and integers y such that

$$p_1 \ge p_2 \ge p_3; \quad p_1 \ge N^{\alpha}; \quad p_3 \ge N^{\beta}; \quad p_1p_2p_3 \le N^{1-\beta} \tag{52}$$

and

$$y < \frac{N}{p_1p_2p_3}; \quad P(y) \le p_3.$$

Note that if t and T are such that

$$\Big(1-\frac{c}{\log p}\Big)p_3 < t < p_3, \qquad \Big(1-\frac{c}{\log p}\Big)\frac{N}{p_1p_2p_3} < T < \frac{N}{p_1p_2p_3}, \tag{53}$$

where $c > 0$ is any constant, then we can substitute the condition on y with

$$P(y) \le t; \quad y < T \tag{54}$$

by changing the sum (51) with an additional term of size at most

$$\frac{N(\log\log p)^{O(1)}}{\log p}.$$

Thus, for any t and T satisfying (53) we have

$$\Big|\sum_{x\in\mathcal{G}} e_p(ax^*)\Big| < \frac{N(\log\log p)^{O(1)}}{\log p} + \sum_{p_1}\sum_{p_2}\sum_{p_3}\Big|\sum_{y} e_p(ap_1^*p_2^*p_3^*y^*)\Big|,$$

where the summations are taken over primes p_1, p_2, p_3 and integers y satisfying (52) and (54).

Now we split the range of variations of primes p_1, p_2, p_3 into subintervals of the form $[L, L + L(\log p)^{-1}]$ and choosing suitable t and T we obtain that for some numbers M_1, M_2, M_3 with

$$M_1 > 0.5M_2 > 0.2M_3, \quad M_1 > N^{\alpha}, \quad M_3 \geq N^{\beta}, \quad M_1M_2M_3 < N^{1-\beta} \tag{55}$$

one has

$$\begin{aligned}\Big|\sum_{x\in\mathcal{G}} e_p(ax^*)\Big| < \frac{N(\log\log p)^{O(1)}}{\log p} \\ + (\log p)^{10}\sum_{p_1\in I_1}\sum_{p_2\in I_2}\sum_{p_3\in I_3}\Big|\sum_{\substack{y\leq M\\ P(y)\leq M_3}} e_p(ap_1^*p_2^*p_3^*y^*)\Big|,\end{aligned} \tag{56}$$

where

$$I_j = \Big[M_j, M_j + \frac{M_j}{\log p}\Big], \qquad M = \frac{N}{M_1M_2M_3} \geq N^{\beta}.$$

Denote

$$W = \sum_{p_1\in I_1}\sum_{p_2\in I_2}\sum_{p_3\in I_3}\Big|\sum_{\substack{y\leq M\\ P(y)\leq M_3}} e_p(ap_1^*p_2^*p_3^*y^*)\Big|.$$

Applying the Cauchy-Schwarz inequality, we get

$$W^2 \leq M_1M_2M_3\sum_{y\leq M}\sum_{z\leq M}\Big|\sum_{p_1\in I_1}\sum_{p_2\in I_2}\sum_{p_3\in I_3} e_p\Big(ap_1^*p_2^*p_3^*(y^*-z^*)\Big)\Big|.$$

Taking into account the contribution from $y = z$ and then fixing $y \neq z$ we get, for some $b \not\equiv 0 \pmod p$,

$$W^2 \leq \frac{N^2}{M} + NM|S|, \tag{57}$$

where

$$|S| = \Big|\sum_{p_1\in I_1}\sum_{p_2\in I_2}\sum_{p_3\in I_3} e_p(bp_1^*p_2^*p_3^*)\Big|.$$

Define integers k_1, k_2, k_3 such that

$$p^{\frac{1}{2k_j}} \leq M_j < p^{\frac{1}{2(k_j-1)}}, \quad j = 1, 2, 3.$$

From (55) and the choice of α and β, it follows, in particular, that

$$k_1 < \frac{1}{\varepsilon\alpha} < (\log p)^{1/2}, \quad k_2, k_3 < \frac{1}{\varepsilon\beta} < (\log p)^{1/2}. \tag{58}$$

We further take even integers $l_j \in \{k_j, k_j+1\}, \quad (j = 1, 2, 3)$ and define

$$\eta_j(\lambda) = \Big|\{(x_1, \ldots, x_{l_j}) \in (I_j \cap \mathcal{P})^{l_j} : x_1^* - x_2^* + \ldots - x_{l_j}^* \equiv \lambda \pmod p\}\Big|.$$

We have

$$\sum_{\lambda=0}^{p-1} \eta_j(\lambda) < M_j^{l_j} \tag{59}$$

and, applying Theorem 6,

$$\begin{aligned}\sum_{\lambda=0}^{p-1} \eta_j(\lambda)^2 <& M_j^{2(l_j-k_j)} M_j^{k_j} (2k_j)^{k_j} \Big(\frac{M_j^{2k_j-1}}{p} + 1\Big) \\ <& (2k_j)^{k_j} M_j^{2l_j} p^{-1/2}.\end{aligned} \tag{60}$$

Next we apply consequently the Hölder inequality. We get

$$|S|^{l_1} < (M_2M_3)^{l_1-1} \sum_{p_2\in I_2} \sum_{p_3\in I_3} \Big|\sum_{p_1\in I_1} e_p(bp_1^*p_2^*p_3^*)\Big|^{l_1}$$

and since we took l_j even, we further get

$$\begin{aligned}|S|^{l_1} <& (M_2M_3)^{l_1-1} \sum_{\lambda_1=0}^{p-1} \eta_1(\lambda_1) \Big[\sum_{p_2\in I_2} \sum_{p_3\in I_3} e_p(b\lambda_1 p_2^* p_3^*)\Big] \\ <& (M_2M_3)^{l_1-1} \sum_{\lambda_1=0}^{p-1} \eta_1(\lambda_1) \sum_{p_3\in I_3} \Big|\sum_{p_2\in I_2} e_p(b\lambda_1 p_2^* p_3^*)\Big|.\end{aligned}$$

Applying the Hölder inequality and using (59), we obtain

$$\begin{aligned}|S|^{l_1l_2} <& (M_2M_3)^{(l_1-1)l_2} M_1^{(l_2-1)l_1} M_3^{l_2-1} \sum_{\lambda_1=0}^{p-1} \eta_1(\lambda_1) \sum_{p_3\in I_3} \Big|\sum_{p_2\in I_2} e_p(b\lambda_1 p_2^* p_3^*)\Big|^{l_2} \\ =& M_1^{l_1(l_2-1)} M_2^{l_2(l_1-1)} M_3^{l_1l_2-1} \sum_{\lambda_1=0}^{p-1} \sum_{\lambda_2=0}^{p-1} \eta_1(\lambda_1)\eta_2(\lambda_2) \Big|\sum_{p_3\in I_3} e_p(b\lambda_1\lambda_2 p_3^*)\Big|.\end{aligned}$$

We again apply the Hölder inequality and use (59),

$$\begin{aligned}|S|^{l_1l_2l_3} &< M_1^{l_1l_3(l_2-1)}M_2^{l_2l_3(l_1-1)}M_3^{l_3(l_1l_2-1)}(M_1^{l_1}M_2^{l_2})^{l_3-1}\times\\ &\times\Big|\sum_{\lambda_1=0}^{p-1}\sum_{\lambda_2=0}^{p-1}\sum_{\lambda_3=0}^{p-1}\eta_1(\lambda_1)\eta_2(\lambda_2)\eta_3(\lambda_3)e_p(b\lambda_1\lambda_2\lambda_3)\Big|\\ &= M_1^{l_1l_2l_3-l_1}M_2^{l_1l_2l_3-l_2}M_3^{l_1l_2l_3-l_3}|S_1|,\end{aligned}$$

where

$$|S_1| = \Big|\sum_{\lambda_1=0}^{p-1}\sum_{\lambda_2=0}^{p-1}\sum_{\lambda_3=0}^{p-1}\eta_1(\lambda_1)\eta_2(\lambda_2)\eta_3(\lambda_3)e_p(b\lambda_1\lambda_2\lambda_3)\Big|.$$

We apply Lemma 1 with $n=3$ and

$$\gamma_j(\lambda) = \frac{\eta_j(\lambda)}{M^{l_j}}.$$

From (59) it follows that

$$\|\gamma_i\|_1 = \sum_{\lambda=0}^{p-1}\frac{\eta_j(\lambda)}{M^{l_j}} \le 1.$$

From (60) and (58) it follows that

$$\|\gamma_i\|_2 = \Big(\sum_{\lambda=0}^{p-1}\Big(\frac{\eta_j(\lambda)}{M^{l_j}}\Big)^2\Big)^{1/2} < p^{-1/5},$$

and, in particular,

$$\prod_{i=1}^{n}\|\gamma_i\|_2 < p^{-1/2-1/10}.$$

Thus, Lemma 1 applies and leads to

$$|S_1| < M_1M_2M_3p^{-c},$$

for some absolute constant $c>0$. Consequently

$$|S| < M_1M_2M_3p^{-c_1/(k_1k_2k_3)} < M_1M_2M_3m^{-c_2\varepsilon^3\alpha\beta^2}.$$

Inserting this into (57) and taking into account that

$$M > N^\beta = p^{\varepsilon\beta} > \exp(\sqrt{\log p}),$$

we get

$$W < \frac{N}{\exp(0.5\sqrt{\log p})} + Nm^{-c_3\varepsilon^3\alpha\beta^2}.$$

Inserting this into (56), we get

$$\Big|\sum_{x\in\mathcal{G}} e_p(ax^*)\Big| < \frac{N(\log\log p)^{O(1)}}{\log p} + (\log p)^{10} Nm^{-c_3\varepsilon^3\alpha\beta^2}.$$

Therefore

$$\Big|\sum_{x<N} e_p(ax^*)\Big| \le \frac{N(\log\log p)^{O(1)}}{\log p} + 12\beta(\log\log p)^2 N + (\log p)^{10} Nm^{-c_3\varepsilon^3\alpha\beta^2}.$$

Thus, taking

$$\beta = \frac{C\log\log p}{\varepsilon^{3/2}(\log p)^{1/2}},$$

with sufficiently large constant C, we obtain

$$\Big|\sum_{x<N} e_p(ax^*)\Big| \ll \frac{(\log\log p)^3}{(\log p)^{1/2}}\,\varepsilon^{-3/2}N,$$

which finishes the proof.

12.3 Proof of Theorem 17

We only treat the case when q is prime, but the argument generalizes.

We follow [17]. Denote

$$\begin{aligned}
&\mathcal{A} = \{n \le x;\ n \equiv a \pmod q\},\\
&\mathcal{A}_d = \{n \in \mathcal{A};\ n \equiv 0 \pmod d\},\\
&S(\mathcal{A}, z) = |\{n \in \mathcal{A};\ (n,p) = 1 \text{ for } p < z, (p,q) = 1\}|,\\
&D = \frac{x^{1-\varepsilon}}{q}.
\end{aligned}$$

Let $D^{1/5} < w < y < z = (x/q)^{1/3}$, where w and y to specify, and write using Buchstab's identity

$$\begin{aligned}
S(\mathcal{A}, z) = &S(\mathcal{A}, w) - \sum_{y\le p<z} S(\mathcal{A}_p, z) - \sum_{w\le p<y} S(\mathcal{A}_p, w)\\
&+ \sum_{w\le p_1<p_2<y} S(\mathcal{A}_{p_1p_2}, p_2).
\end{aligned} \tag{61}$$

Applying the basic estimates of the linear sieve on each of the terms in (61) leads to the bound

$$S(\mathcal{A}, z) < \frac{2x}{\phi(q)\log D}, \tag{62}$$

see the discussion in [17] and also [18, p.265]. In particular this involves bounding

$$S(\mathcal{A}_{p_1p_2}, p_2) < \frac{2x}{\phi(q)p_1p_2\log D_{12}} \quad \text{with} \quad D_{12} = \frac{D}{p_1p_2}. \tag{63}$$

Here D_{12} is the level of distribution for the sequence $\mathcal{A}_{p_1p_2}$. The idea from [17] is to improve on (63), in the average over p_1, p_2, by increasing the level D_{12} to some level D'_{12}.

More precisely, define the reminders

$$R_{p_1,p_2,d} = |\mathcal{A}_{dp_1p_2}| - \frac{x}{qdp_1p_2} \tag{64}$$

that appear as the error terms in the sieving process. The strategy is to bound the collected contribution of $R_{p_1,p_2,d}$, performing the summation over p_1, p_2.

Subdivide $[w, y]$ in dyadic ranges and estimate

$$\sum_{\substack{p_1\sim P_1\\ p_2\sim P_2}} S(\mathcal{A}_{p_1p_2}, p_2)$$

for fixed P_1, P_2. We introduce $D'_{12} = D'_{12}(P_1, P_2) > D_{12}$ such that

$$\sum_{d<D'_{12}} \Big|\sum_{\substack{p_1\sim P_1\\ p_2\sim P_2}} R_{p_1,p_2,d}\Big| < \frac{x^{1-\varepsilon}}{q}\, P_1P_2. \tag{65}$$

With D'_{12} as sieving limit, (63) improves to

$$S(\mathcal{A}_{p_1p_2}, p_2) < \frac{2x}{\phi(q)p_1p_2\log D'_{12}}$$

on average over $p_1 \sim P_1$, $p_2 \sim P_2$, provided $p_2^3 > D'_{12}$. The gain in (62) becomes then of the order

$$\begin{aligned}&\frac{x}{\phi(q)} \sum_{w\le p_1<p_2<y} \frac{1}{p_1p_2}\Big(\frac{1}{\log D_{12}} - \frac{1}{\log D'_{12}(p_1, p_2)}\Big)\\ &\le \frac{x}{\phi(q)} \sum_{w\le p_1<p_2<y} \frac{1}{p_1p_2}\,\frac{\log\frac{D'_{12}(p_1,p_2)}{D_{12}}}{(\log D_{12})^2}.\end{aligned} \tag{66}$$

Using the analysis from [17] in order to express (64) as exponential sums, we obtain following bound on the left hand side of (65)

$$\sum_{d<D'_{12}} \sum_{0<|h|<H} \Big| \sum_{\substack{p_1 \sim P_1 \\ p_2 \sim P_2}} (qdp_1p_2)^{-1} \widehat{f}\Big(\frac{h}{qdp_1p_2}\Big) e_q(-ahd^* p_1^* p_2^*) \Big| \tag{67}$$

up to admissible error term. Here

$$H = qdP_1P_2x^{2\varepsilon-1}$$

and $f \geq 0$ is supported on $x^{1-\varepsilon} < t < x + x^{1-\varepsilon}$ satisfying $\widehat{f}(0) = x$ and $t^j f^{(j)}(t) \ll x^\varepsilon$ for $j \geq 0$. Standard manipulations permit to express (67) in terms of trilinear sums ($D_{12} \leq \widetilde{D} < D'_{12}$)

$$\frac{x}{q\widetilde{D}P_1P_2} H \Big| \sum_{\substack{d \in I_0 \\ p_1 \in I_1 \\ p_2 \in I_2}} \alpha_d \beta_{p_1} \gamma_{p_2} e_q(-ahd^* p_1^* p_2^*) \Big|$$

with $|\alpha_d|, |\beta_{p_1}|, |\gamma_{p_2}| \leq 1$ and

$$I_0 \subset [\widetilde{D}, 2\widetilde{D}], \quad I_1 \subset [P_1, 2P_1], \quad I_2 \subset [P_2, 2P_2]$$

intervals. Note that these intervals always be enlarged to

$$I_0 = [\widetilde{D}, 2\widetilde{D}], \quad I_1 = [P_1, 2P_1], \quad I_2 = [P_2, 2P_2].$$

Take $\delta = (1-\theta)/5$ and $w = x^\delta$, $y = x^{2\delta}$. Note that

$$\widetilde{D} > D_{12} > \frac{D}{y^2} > x^{0.9\delta}.$$

Performing the Karatsuba amplification followed by a trilinear estimate gives a saving of a factor $x^{c'\delta^3}$, hence

$$\frac{x}{q\widetilde{D}P_1P_2} H \Big| \sum_{\substack{d \in I_0 \\ p_1 \in I_1 \\ p_2 \in I_2}} \alpha_d \beta_{p_1} \gamma_{p_2} e_q(-ahd^* p_1^* p_2^*) \Big| < \frac{x^{1-c'\delta^3}}{q} H < x^{2\varepsilon - c'\delta^3} D'_{12} P_1 P_2$$

which is less than $x^{1-\varepsilon} q^{-1}$ for

$$D'_{12} = \frac{x^{1+c''\delta^3}}{qP_1P_2} = D_{12} x^{c''\delta^3}.$$

The condition $w^5 > D'_{12}$ is satisfied. Thus, returning to (66), we obtain the saving

$$\frac{x}{\phi(q)} \sum_{x^\delta < p_1 < p_2 < x^{2\delta}} \frac{1}{p_1 p_2} \frac{\log(x^{c''\delta^3})}{\delta^2 (\log x)^2} \gg \frac{x\delta}{\phi(q)\log x} \sim \frac{x\delta^2}{\phi(q)\log \frac{x}{q}}$$

and since ε is arbitrarily small, the result follows.

13 Comments

There is an alternative approach to Theorem 17 following the proof of [18, Theorem 13.1]. On [18, p.262], there is a bound

$$R(M,N) \ll x^\varepsilon \Big\{(M,N) - \text{bilinear Kloosterman sum}\Big\} + \frac{x^{1-\varepsilon}}{q}.$$

According to [18, Theorem 12.21], we may consider any factorization $D = MN$. Let $x/q = x^\delta$ and take k such that

$$\frac{1}{2k-1} \leq \frac{\delta}{2} < \frac{1}{2k-3}.$$

Let

$$N = q^{1/(2k-1)}, \quad M = \frac{D}{N}.$$

From our Theorem 8 it follows that

$$\Big\{(M,N) - \text{bilinear Kloosterman sum}\Big\} < MN^{1-c/k^2} < D^{1-c\delta^2}.$$

From condition $D^{1-c\delta^2} < x^{1-\varepsilon}q^{-1}$ we obtain,

$$\pi(x;q,a) < \frac{(2-c\delta^2)x}{\phi(q)\log(x/q)}.$$

As we have mentioned in the introduction one can prove that if $I \subset \mathbb{F}_p^*$ with $|I| < p^{1/2}$, then

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{1.55+o(1)}.$$

This is better than what one gets from Corollary 1 for $k = 3$. Let us prove this bound. We can assume that $|I| = N > p^{1/3}$, as Corollary 4 implies a better bound

$$|I^{-1} + I^{-1}| > |I|^{2+o(1)}.$$

Consider the congruence

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} \equiv \frac{1}{x_4} + \frac{1}{x_5} + \frac{1}{x_6} \pmod p, \quad x_1, \dots, x_6 \in I.$$

The number J_6 of this congruence can be bounded by

$$J_6 \leq (J_4 J_8)^{1/2}.$$

From Theorem (1) it follows that $J_8 < N^{32/5+o(1)}$, and from Corollary 4 we have that

$$J_4 < \frac{N^{7/2+o(1)}}{p^{1/2}}.$$

Thus,

$$J_6 < \frac{N^{99/20+o(1)}}{p^{-1/4}}.$$

Using the relationship between the number of solutions of a congruence and the cardinality of the corresponding set, we conclude that

$$|I^{-1} + I^{-1} + I^{-1}| \geq N^{21/20+o(1)} p^{1/4} > N^{1.55+o(1)}.$$

We remark that the arguments in the proof of Theorem 1 also give the following.

Proposition 1. *For any fixed positive integer constants r and k the number $J_{2k}^{(r)}$ of solutions of the congruence*

$$\frac{1}{x_1^r} + \ldots + \frac{1}{x_k^r} \equiv \frac{1}{x_{k+1}^r} + \ldots + \frac{1}{x_{2k}^r} \pmod p, \qquad x_1, \ldots, x_{2k} \in I,$$

satisfies the bound

$$J_{2k}^{(r)} < \Big(|I|^{2k^2/(k+1)} + \frac{|I|^{2k}}{p}\Big)|I|^{o(1)}.$$

Thus, in particular we obtain

Corollary 5. *Let r_1, r_2, k_1, k_2 be fixed positive integer constants, $I_1 = [a_1 + 1, a_1 + N_1]$, $I_2 = [a_2 + 1, a_2 + N_2]$ and*

$$N_1 < p^{\frac{k_1+1}{2k_1}}, \quad N_2 < p^{\frac{k_2+1}{2k_2}}.$$

Then for any complex coefficients $\alpha_1(x_1), \alpha_2(x_2)$ with $|\alpha_i(x_i)| \le 1$ one has

$$\max_{(a,p)=1}\Big|\sum_{x_1\in I_1}\sum_{x_2\in I_2}\alpha_1(x_1)\alpha_2(x_2)e_p(ax_1^{-r_1}x_2^{-r_2})\Big| < \Big(p^{\frac{1}{2k_1k_2}}N_1^{-\frac{1}{k_2(k_1+1)}}N_2^{-\frac{1}{k_1(k_2+1)}}\Big)(N_1N_2)^{1+o(1)}.$$

One may apply the bilinear sums of Corollary 5 together with Vaughan's formula [32] to bound the corresponding sums over primes, similar to those in [5, Theorems A1, A9] and [14, Corollary 1.5].

Corollary 6. *Let $r \in \mathbb{Z}_+$ and $p > N > p^{1/2+\varepsilon}$ for some $\varepsilon > 0$. Then*

$$\max_{(a,p)=1}\Big|\sum_{\substack{x<N\\ x \text{ prime}}} e_p(ax^{-r})\Big| < N^{1-\delta}$$

for some $\delta = \delta(\varepsilon; r) > 0$.

Next we remark that the result from [19] implies the bound

$$\max_{(a,p)=1}\Big|\sum_{\substack{x<p\\ x \text{ prime}}} e_p(ax^{-1})\Big| < p^{15/16+o(1)}.$$

Our Corollary 5 leads to

Corollary 7. *For any fixed positive integer constant r the following bound holds:*

$$\max_{(a,p)=1}\Big|\sum_{\substack{x<p\\ x \text{ prime}}} e_p(ax^{-r})\Big| < p^{23/24+o(1)}.$$

Let us prove it. It suffices to establish the bound

$$\Big|\sum_{n\le p}\Lambda(n)e_p(an^{-r})\Big| < p^{23/24+o(1)}$$

and then the result follows by partial summation. Here $\Lambda(n)$ is the Mangoldt function.

Below we use $A \lessapprox B$ to mean that $A < Bp^{o(1)}$. From the Vaughan's identity (see [13, Chapter 24]), we have

$$\sum_{n\le p} \Lambda(n) e_p(an^{-r}) \lessapprox W_1 + W_2 + W_3 + W_4,$$

where

$$\begin{aligned} W_1 &= \Big|\sum_{n\le U} \Lambda(n) e_p(an^{-r})\Big|; \\ W_2 &= \sum_{n\le UV} \Big|\sum_{m\le p/n} e_p(an^{-r}m^{-r})\Big|; \\ W_3 &= \sum_{n\le V} \Big|\sum_{m\le p/n} (\log m) e_p(an^{-r}m^{-r})\Big|; \\ W_4 &= \sum_{U<n\le p/V} \Big|\sum_{V<m\le p/n} \beta_m e_p(an^{-r}m^{-r})\Big|. \end{aligned}$$

Here $U \ge 2, V \ge 2$ are parameters with $UV \le p$,

$$\beta_m = \sum_{\substack{d|m \\ d\le V}} \mu(d).$$

Below we shall also use Weil's bound of the form

$$\Big|\sum_{x=1}^{p-1} e_p(ax^{-r} + bx)\Big| \ll p^{1/2}.$$

More precisely, we shall use a consequence of this bound, namely if I is an interval in $\mathbb{F}_p$ then

$$\Big|\sum_{x\in I} e_p(ax^{-r})\Big| \lessapprox p^{1/2}.$$

We take $U = V = p^{1/3}$ and estimate W_1 trivially:

$$W_1 \lessapprox U = p^{1/3}.$$

To estimate W_2 we split the range of summation over n into dyadic intervals and get, for some $L \le p^{2/3}$,

$$W_2 \lessapprox \sum_{L \le n \le 2L} \Big| \sum_{m \le p/n} e_p(an^{-r}m^{-r}) \Big|.$$

If $L < p^{1/3}$ then we apply Weil's bound to the sum over m and get

$$W_2 \lessapprox Lp^{1/2} \lessapprox p^{5/6}.$$

If $p^{1/3} < L < p^{2/3}$ then using the standard smoothing argument we extend the summation over m to $m \le p/L$ and apply Corollary 5 with $k_1 = k_2 = 2$ to get

$$W_2 \lessapprox p^{23/24}.$$

To estimate W_3 we use partial summation (to the sum over m) and Weil's bound and get

$$W_3 \lessapprox \sum_{n < p^{1/3}} p^{1/2} \lessapprox p^{5/6}.$$

To estimate W_4, we split the range of summation over n into dyadic intervals and get, for some $p^{1/3} < L \le p^{2/3}$,

$$W_4 \lessapprox \sum_{L \le n < 2L} \Big| \sum_{p^{1/3} < m \le p/n} \beta_m e_p(an^{-r}m^{-r}) \Big|.$$

Applying the smoothing argument to extend the sum over m to $m < p/L$ and using Corollary 5 with $k_1 = k_2 = 2$, we get

$$W_4 \lessapprox p^{23/24}$$

and Corollary 7 follows.

References

[1] A. Ayyad, T. Cochrane and Z. Zheng, 'The congruence $x_1x_2 \equiv x_3x_4 \pmod{p}$, the equation $x_1x_2 = x_3x_4$ and the mean value of character sums', *J. Number Theory*, **59** (1996), 398–413.

[2] R. C. Baker, 'Kloosterman sums with prime variable', *Acta Arith.*, (to appear).

[3] U. Betke, M. Henk and J. M. Wills, 'Successive-minima-type inequalities', *Discr. Comput. Geom.*, **9** (1993), 165–175.

[4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.

[5] J. Bourgain, 'More on sum-product phenomenon in prime fields and its applications', *Int. J. Number Theory* **1** (2005), 1–32.

[6] J. Bourgain, 'Multilinear exponential sums in prime fields under optimal entropy condition on the sources', *Geom. Funct. Anal.* **18** (2009), 1477–1502.

[7] J. Bourgain, 'The discretized sum-product and projection theorems', *J. Anal. Math.* **112** (2010), 193–236.

[8] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On the hidden shifted power problem', *SIAM J. Comp.*, (to appear).

[9] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Inst. Math.* (to appear).

[10] N. G. de Bruijn, 'On the number of positive integers $\le x$ and free prime factors $> y$, II', *Indag. Math.* **28** (1966), 239-247.

[11] D. A. Burgess, 'Partial Gaussian sums', *Bull. London Math. Soc.*, **20** (1988), 589–592.

[12] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Geom. Func. Anal.*, **21** (2011), 892–904.

[13] H. Davenport, "Multiplicative Number Theory". Third edition, revised by H. L. Montgomery. Springer-Verlag, New York, 2000.

[14] E. Fouvry and Ph. Michel 'Sur certaines sommes d'exponentielles sur les nombres premiers', *Ann. Sci. cole Norm. Sup.* **31** (1998), 93–130.

[15] E. Fouvry and I. E. Shparlinski 'On a ternary quadratic form over primes', *Acta Arith.* **150** (2011), 285–314.

[16] J. Friedlander and H. Iwaniec, 'Estimates for character sums', *Proc. Amer. Math. Soc.*, **119** (1993), 365–372.

[17] J. Friedlander and H. Iwaniec, *The Brun-Titchmarsh theorem*, *Analytic number theory* (Kyoto, 1996), 85-93, London Math. Soc. Lecture Note Ser., 247, Cambridge Univ. Press, Cambridge, 1997.

[18] J. Friedlander and H. Iwaniec, *Opera de Cribro*, American Mathematical Society, Colloquium Publications, 57, 2010.

[19] M. Z. Garaev, 'Estimation of Kloosterman sums with primes and its application', *Math. Notes* **88**:3 (2010), 365–373.

[20] D. R. Heath-Brown, 'Almost-primes in arithmetic progressions and short intervals', *Math. Proc. Cambridge Philos. Soc.* **83** (1978), no. 3, 357–375.

[21] M. N. Huxley, 'On the difference between consecutive primes', *Invent. Math.* **15** (1972), 164-170.

[22] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer, 1990.

[23] A. A. Karatsuba, 'New estimates of short Kloosterman sums', *Math. Notes* **88**:3 (2010), 347–359. Prepared by E. A. Karatsuba, M. A. Korolev and I. S. Rezvyakova on notes and drafts of A. A. Karatsuba.

[24] A. A. Karatsuba, 'Analogues of Kloosterman sums', *Izv. Math.* **59**:5 (1995), 971–981.

[25] A. A. Karatsuba, 'Fractional parts of functions of a special form', *Izv. Math.* **59**:4 (1995), 721–740.

[26] M. A. Korolev, 'Incomplete Kloosterman sums and their applications', *Izv. Math.* **64**:6 (2000), 1129-1152.

[27] M. A. Korolev, 'Short Kloosterman sums with weights', *Math. Notes* **88**:3 (2010), 374-385.

[28] W. Luo, 'Bounds on incomplete multiple Kloosterman sums', *J. Number Theory*, **75** (1999), 41–46.

[29] V. V. Prasolov, *Polynomials*, Algorithms and Computation in Mathematics, **11**, Springer-Verlag, Berlin, 2004.

[30] I. E. Shparlinski, 'Bounds on incomplete multiple Kloosterman sums', *J. Number Theory*, **126** (2007), 68–73.

[31] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge University Press, Cambridge, 2006.

[32] R. C. Vaughan, 'Sommes trigonométriques sur les nombres premiers', *C.R. Acad. Sci. Paris* Ser. A **285**, 981-983.